Data & Communications Working Group of the IBA Communication Law Committee

Data localisation guide: A report on global data isolationism

Introduction

The Data & Communications Working Group of the IBA Communications Law Committee

The Data & Communications Working Group ("Working group") of the IBA Communications Law Committee focuses on the intersection of the regulation of data and communications. Its work will cover issues such as privacy for communications, Big Data, access to data & communications, personal and non-personal data regulation, cybersecurity and the free flow of data/data localisations.

The Members of the Working Group come from private practice, in-house and national regulatory authorities around the globe. The 2018/2019 members of the Data & Communications Working Group that contributed to this report are:

- Charles Coorey (Chair), Gilbert + Tobin, Sydney, Australia;
- Juan Enrique Allard, Guerrero Olivos, Santiago, Chile;
- Pascal Dutru, Communication Regulatory Authority of Qatar, Doha, Qatar; and
- Philippe Vogeleer, Vodafone, London, United Kingdom.

The work of the Working Group has been supported by relevant officers of the IBA Communications Law Committee, namely Laurent De Muyter, Jones Day, Brussels, Belgium and Jana Pattynova, Pierstone, Prague, Czech Republic.

This publication

The purpose of this inaugural publication of the Working Group is to provide for a tool comparing the data localisation regimes that exist in various countries around the world. This publication was chosen as the Working Group's inaugural publication because:

- of the currency of the topic;
- its cross-jurisdictional appeal;
- the common view that greater understanding was required of the theme of "isolationism in data" due to the proliferation of seemingly differing regimes, even with the global regime; and
- in light of the point above, the difficulties experienced by:
  - corporations in making foreign investment decisions with confidence; and
  - lawyers in advising their clients on such decisions.

To achieve this purpose the Members of the Data & Communications Working Group identified 13 questions and compiled responses as the foundation for the international comparison. The questions are contained in the table below. The responses are provided per country in the annex.

1	What is the relevant legislation? Are general data protection laws the only relevant laws or are there other sector specific laws as well that may impose additional requirements?
2	Are there any bills currently before parliament, or expected to come before parliament, that propose to amend the existing regime?
3	What type of approach is this? • Consumer protection led? • Other?
4	What is the scope of the law? • Telecoms? • Social media? • Media? • Medical? • Banking? • Other?
5	What does it imply in terms of data collection? • Do all types of data need to be captured, or only personal data? How are they categorised? • Is the data stored by the commercial entity or by a public entity? • Is the data copied / sent to a public entity?
6	What does it imply in terms of data storage? • Does data have to be stored locally? • Can data be stored outside of the country? • Can data stored locally be exported outside of the country? • Does that require an authorisation? • If so, by whom?

7	What does it imply in terms of data processing? • Do the same processes apply to all data, or only to personal data? • Are these processes same for technical and commercial usage? • Can data be processed abroad? If so, does the data processor have to give mirror access locally? • How long is the data stored? • Is the data destructed after that period of time, or kept? • Is that monitored independently, or only by the State?
8	What does it imply in terms of data usage? • Can data be sold? • Can statistical data be sold? • Can technical data be sold?
9	What control do people have on their data? • Are people informed of the data being collected? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) as a bulk? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) line by line? • How is that approval stored? • Who monitors it?
10	Who is responsible for the implementation of the law? • NRA? • Ministry of ICT? • Army (or affiliate)? • Other?
11	Who is responsible for possible breaches to the law? • Users? • Service provider?

	• Local operator? Just for themselves, or also on behalf of their counterparts? • Foreign operator / data handler?
12	Implications of breach • Risks to companies – Penalties – Loss of license – Other • Risks to people – Penalties – Arrest – Other
13	Who monitors the correct implementation of the law? • Parliament? • Consumer associations / civil society? • Nobody? • Other?

The Members of the Data & Communications Working Group considered that this publication could become an important resource that:

- makes a meaningful contribution to data localisation jurisprudence; and
- can be accessed and cited by the legal community regardless of which firm they work at or which country they practice in.

This publication is also intended to be a "living document" as what has been included in this inaugural version is merely the starting point for further contributions for other countries and for more detail within countries.

Jurisdictions included in this publication

The jurisdictions covered in this inaugural publication are listed below.

Africa	*Asia Pacific*	*Europe*	*South and central America*
Egypt	Australia	European Union	Argentina

Ghana	China		Brazil
Lesotho	India		Chile
South Africa	Indonesia		Colombia
Tanzania	Japan		Mexico
	Singapore		Peru
	South Korea		Uruguay

Additional jurisdictions, including the Gulf Cooperation Council and Russia, will be added to this publication in due time.

The members of the Working Group wish to thank their immediate colleagues for their assistance and would like to especially acknowledge the contributions made by their broader colleagues from the following firms:

- Marval, O'Farrell & Mairal (Argentina);
- Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados (Brazil);
- Posse Herrera Ruiz (Colombia);
- Creel, García-Cuéllar, Aiza y Enríquez (Mexico);
- Rodrigo, Elías & Medrano (Peru); and
- Hughes & Hughes (Uruguay).

Initial two key themes

The 13 questions posed across the jurisdictions clearly allow for a range of findings to be made and users of this resource are encouraged to explore and cross-reference the responses.

To point out two key themes that have been initially identified:

- the overwhelming majority of countries included in this inaugural work have consumer protection-led data localisation regimes. The only exceptions are:
  - China, where the regime is national security-led;
  - Lesotho, where the regime is government-led; and
  - Tanzania, where there is no law governing data protection; and
- the scope of laws is very broad, but jurisdictions can be broadly grouped as follows:
  - overarching personal data regime: Argentina, Australia, Brazil (upcoming), Chile, Colombia, Egypt, European Union, Ghana, India (upcoming), Indonesia (upcoming), Japan, Lesotho, Mexico, Peru, Singapore, South Africa, South Korea and Uruguay;

- banking/finance specific: Australia, Chile, China, Colombia, European Union, Ghana and Singapore;
- cybercrime / cybersecurity specific: China and Egypt;
- healthcare specific: Australia, China and the European Union; and
- telecommunications specific: Argentina, Australia, China, Egypt, European Union, Ghana, India and Singapore.

Moving forward

As mentioned earlier, it is the intention of the members of this Working Group that this resource will continue to evolve. The members encourage you to continue to revisit this resource for the latest updates and warmly welcome your feedback on the continued development of this resource.

Africa

Country: Egypt

Questionnaire

#	Question	Response/Yes/No	Comment
1	What is the relevant legislation? Are general data protection laws the only relevant laws or are there other sector specific laws as well that may impose additional requirements?	EU GDPR is N/A for Egypt **Local Applicable Laws/Regulations:** Telecom Laws - Issued Telecom Licence - Issued Cybercrime Law - Issued Personal Data Protection Law – Not Yet	
2	Are there any bills currently before parliament, or expected to come before parliament, that propose to amend the existing regime?	Yes	Personal Data Protection Law – New Law Currently in discussion phase in Egyptian Parliament
3	What type of approach is this? • Consumer protection led?	Telecom Laws - Consumer Protection Led Telecom Licence - Consumer Protection Led	

#	Question	Response/Yes/No	Comment
	• Other?	Cybercrime Law - National Security Led Personal Data Protection Law – Consumer Protection Led	
4	What is the scope of the law? • Telecoms? • Social media? • Media? • Medical? • Banking? • Other?	Telecom Laws - Telecom Telecom Licence - Telecom Cybercrime Law – General Data (Electronic, Personal, Governmental, etc…) across all sectors Personal Data Protection Law – Personal Data across all sectors	
5	What does it imply in terms of data collection? • Do all types of data need to be captured, or only personal data? How are they categorised? • Is the data stored by the commercial entity or by a public entity? • Is the data copied / sent to a public entity?	Can only talk on new Data Protection Law as my area of specialization i.e. not sure about other applicable laws and regulations and answering the below in reference to those laws/regulations would require sometime to run it by proper teams All applicable and covered under new Data Protection Law since it adopts EU GDPR principles	

#	Question	Response/Yes/No	Comment
6	What does it imply in terms of data storage? • Does data have to be stored locally? • Can data be stored outside of the country? • Can data stored locally be exported outside of the country? • Does that require an authorisation? • If so, by whom?	Yes per Telecom License however not mandatory under new Data Protection Law since it adopts EU GDPR principles - conflict to be sorted out after law issuance Not allowed per Telecom License however to be allowed under new Data Protection Law since it adopts EU GDPR principles - conflict to be sorted out after law issuance Yes under new Data Protection Law Cross-Border Transfer Authorization by Data Protection Authority – that is to be established after law issuance	
7	What does it imply in terms of data processing? • Do the same processes apply to all data, or only to personal data? • Are these processes same for technical and commercial usage? • Can data be processed abroad? If so, does the data processor	Can only talk on new Data Protection Law as my area of specialization i.e. not sure about other applicable laws and regulations and answering the below in reference to those laws/regulations would require sometime to run it by proper teams All applicable and covered under new Data Protection Law since it adopts EU GDPR principles	

#	Question	Response/Yes/No	Comment
	have to give mirror access locally? • How long is the data stored? • Is the data destructed after that period of time, or kept? • Is that monitored independently, or only by the State?		
8	What does it imply in terms of data usage? • Can data be sold? • Can statistical data be sold? • Can technical data be sold?	Can only talk on new Data Protection Law as my area of specialization i.e. not sure about other applicable laws and regulations and answering the below in reference to those laws/regulations would require sometime to run it by proper teams All applicable and covered under new Data Protection Law since it adopts EU GDPR principles	
9	What control do people have on their data? • Are people informed of the data being collected? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) as a bulk?	Can only talk on new Data Protection Law as my area of specialization i.e. not sure about other applicable laws and regulations and answering the below in reference to those laws/regulations would require sometime to run it by proper teams All applicable and covered under new Data Protection Law since it adopts EU GDPR principles	

#	Question	Response/Yes/No	Comment
	• Are people capable of accepting (= they want it) or rejecting (= they don't want it) line by line? • How is that approval stored? • Who monitors it?	Data Protection Authority – To be established after DP Law issuance	
10	Who is responsible for the implementation of the law? • NRA? • Ministry of ICT? • Army (or affiliate)? • Other?	Organizations in scope which are monitored by: National Telecom Regulatory Authority – Existing for Telecom Law/License and Cybercrime Law Data Protection Authority – To be established after DP Law issuance	
11	Who is responsible for possible breaches to the law? • Users? • Service provider? • Local operator? Just for themselves, or also on behalf of their counterparts? • Foreign operator / data handler?	All applicable and covered under all laws/regulations i.e. Telecom Law/License, Cybercrime Law and new Data Protection Law	

#	Question	Response/Yes/No	Comment
12	Implications of breach • Risks to companies – Penalties – Loss of license – Other • Risks to people – Penalties – Arrest – Other	All applicable and covered under Cybercrime Law and new Data Protection Law except for Loss of License which is covered under Telecom Law/License	
13	Who monitors the correct implementation of the law? • Parliament? • Consumer associations / civil society? • Nobody? • Other?	Telecom License/Law & Cybercrime → National Telecom Regulatory Authority – Existing DP Law → Data Protection Authority – To be established after DP Law issuance	

Country: Ghana

Questionnaire

#	Question	Response/Yes/No	Comment
1	What is the relevant legislation? Are general data protection laws the only relevant laws or are there other sector specific laws as well that may impose additional requirements?	No	• Data Protection Act, 2012 (Act 843) • Revenue Administration Act, 2016 (Act 915) Relevant National Communications Authority (NCA) legislation
2	Are there any bills currently before parliament, or expected to come before parliament, that propose to amend the existing regime?	No	
3	What type of approach is this? • Consumer protection led? • Other?	N/A	
4	What is the scope of the law? • Telecoms? • Social media? • Media?	N/A	• Data Protection Act: covers personal data • Revenue Administration Act: covers tax. Section 27 provides scope for data retention. Relevant NCA legislation

#	Question	Response/Yes/No	Comment
	• Medical? • Banking? • Other?		
5	What does it imply in terms of data collection? • Do all types of data need to be captured, or only personal data? How are they categorised? • Is the data stored by the commercial entity or by a public entity? • Is the data copied / sent to a public entity?		• Data Protection Act covers personal data Entities store data that is generated unless directed by legislation, policy or industry practice.
6	What does it imply in terms of data storage? • Does data have to be stored locally? • Can data be stored outside of the country? • Can data stored locally be exported outside of the country? • Does that require an authorisation? • If so, by whom?	Yes Yes Yes No	• That is a decision for data controllers to make. In a country with par or higher data protection laws In a country with par or higher data protection laws

#	Question	Response/Yes/No	Comment
7	What does it imply in terms of data processing? • Do the same processes apply to all data, or only to personal data? • Are these processes same for technical and commercial usage? • Can data be processed abroad? If so, does the data processor have to give mirror access locally? • How long is the data stored? • Is the data destructed after that period of time, or kept? • Is that monitored independently, or only by the State?	No No Yes	• Applicable only to personal data • The data processor decides what type of accesses it chooses to give to the controller. • As long as it is necessary and legal to do so Data Processing Agreement and other relevant clauses determine what happens to the data. Act 843 requires that data that is not used should not be retained.
8	What does it imply in terms of data usage? • Can data be sold? • Can statistical data be sold? Can technical data be sold?	No No No	
9	What control do people have on their data?		

#	Question	Response/Yes/No	Comment
	• Are people informed of the data being collected? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) as a bulk? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) line by line? • How is that approval stored? • Who monitors it?	Yes Yes Yes Systems	
10	Who is responsible for the implementation of the law? • NRA? • Ministry of ICT? • Army (or affiliate)? • Other?	• Data Protection Commission • Ministry of Communication	
11	Who is responsible for possible breaches to the law? • Users? • Service provider?	The party through whom the breach occurs either by itself or by third parties.	

#	Question	Response/Yes/No	Comment
	• Local operator? Just for themselves, or also on behalf of their counterparts? • Foreign operator / data handler?		
12	Implications of breach • Risks to companies – Penalties – Loss of license – Other • Risks to people – Penalties – Arrest • Other	 Yes Possible Yes Yes	
13	Who monitors the correct implementation of the law • Parliament? • Consumer associations / civil society? • Nobody? • Other?	Consumer associations and industries	

Country: Lesotho

Questionnaire

#	Question	Response/Yes/No	Comment
1	What is the relevant legislation? Are general data protection laws the only relevant laws or are there other sector specific laws as well that may impose additional requirements?	Yes	The Data Protection Act of Lesotho 2011. The Labour Code Order No: 24 of 1992. The Income Tax Act No:9 of 1993 The Value Added Tax Act No:9 of 2001 Companies Act of Lesotho 2011 Payment System Issuers of Electronic Payment Instruments Regulation 2017.
2	Are there any bills currently before parliament, or expected to come before parliament, that propose to amend the existing regime?	Yes	Data Protection Bill 2013
3	What type of approach is this? • Consumer protection led? • Other?	 Other	It is a government led initiative.
4	What is the scope of the law?		It has an overarching application

#	Question	Response/Yes/No	Comment
	• Telecoms? • Social media? • Media? • Medical? • Banking? • Other?		
5	What does it imply in terms of data collection? • Do all types of data need to be captured, or only personal data? How are they categorised? • Is the data stored by the commercial entity or by a public entity? • Is the data copied / sent to a public entity?	 No	Personal Data, there is no categorization of the data. By the commercial entity. The data is not sent to a public entity, unless we are authorized under the law for law enforcement purposes.
6	What does it imply in terms of data storage? • Does data have to be stored locally? • Can data be stored outside of the country?	 Yes Yes Yes	 But such storage has to be authorised But it has to be subject to the law.

#	Question	Response/Yes/No	Comment
	• Can data stored locally be exported outside of the country? • Does that require an authorisation? • If so, by whom?	Yes The regulator or the data subject.	The regulator or the data subject.
7	What does it imply in terms of data processing? • Do the same processes apply to all data, or only to personal data? • Are these processes same for technical and commercial usage? • Can data be processed abroad? If so, does the data processor have to give mirror access locally? • How long is the data stored? • Is the data destructed after that period of time, or kept? • Is that monitored independently, or only by the State?	Yes Yes Yes Yes	The processing in the Act only refers to personal data. The processor is obliged to give mirror access to us. It depends on the specific sector law. It depends on the specific sector law. By both parties
8	What does it imply in terms of data usage? • Can data be sold? • Can statistical data be sold?	No No	This is not authorised under the Law.

#	Question	Response/Yes/No	Comment
	• Can technical data be sold?	No	
9	What control do people have on their data? • Are people informed of the data being collected? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) as a bulk? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) line by line? • How is that approval stored? • Who monitors it?	Yes Yes Yes	It depends of the type of personal data to be collected and the specific laws. It is technically stored Privacy officer and security officer.
10	Who is responsible for the implementation of the law? • NRA? • Ministry of ICT? • Army (or affiliate)? • Other?		The sector specific regulators are the ones responsible for the implementation of the law.
11	Who is responsible for possible breaches to the law?		All the mentioned parties maybe responsible

#	Question	Response/Yes/No	Comment
	• Users? • Service provider? • Local operator? Just for themselves, or also on behalf of their counterparts? • Foreign operator / data handler?	Yes Yes	
12	Implications of breach • Risks to companies – Penalties – Loss of license – Other • Risks to people – Penalties – Arrest • Other	Yes Yes	All of the mentioned risks maybe possible where there is a breach. All of the mentioned risks maybe possible when a breach occurs.
13	Who monitors the correct implementation of the law? • Parliament? • Consumer associations / civil society?		The sector specific regulators

#	Question	Response/Yes/No	Comment
	• Nobody? • Other?		

Country: South Africa

Questionnaire

#	Question	Response/Yes/No	Comment
1	What is the relevant legislation? Are general data protection laws the only relevant laws or are there other sector specific laws as well that may impose additional requirements?	• Protection of Personal Information Act • Promotion of Access to Information Act • Electronic Communications and Transaction Act • Sector specific Regulations from ICASA (e.g Code of Conduct Regulations)	
2	Are there any bills currently before parliament, or expected to come before parliament, that propose to amend the existing regime?	No	
3	What type of approach is this? • Consumer protection led? • Other?	• Consumer and Enterprise privacy protection	
4	What is the scope of the law?	• Applies to all Responsible Parties processing personal information of Data Subjects	

#	Question	Response/Yes/No	Comment
	• Telecoms? • Social media? • Media? • Medical? • Banking? • Other?		
5	What does it imply in terms of data collection? • Do all types of data need to be captured, or only personal data? How are they categorised? • Is the data stored by the commercial entity or by a public entity? • Is the data copied / sent to a public entity?	• Only personal information and Special Personal Information is captured • Personal information will be stored by commercial entity • In certain instances personal information is disclosed to law enforcement agencies and other government entities subject to the requirements of the law i.e RICA and CPE	
6	What does it imply in terms of data storage?		

#	Question	Response/Yes/No	Comment
	• Does data have to be stored locally? • Can data be stored outside of the country? • Can data stored locally be exported outside of the country? • Does that require an authorisation? • If so, by whom?	• One needs a legal instrument governing transfer of information across the borders of South Africa • There is no need to obtain authorisation	
7	What does it imply in terms of data processing? • Do the same processes apply to all data, or only to personal data? • Are these processes same for technical and commercial usage? • Can data be processed abroad? If so,	• Only personal information is processed • Yes, one needs to adhere to provisions of PoPIA for commercial and technical use • Data can be processed abroad. However, mirror access is not a legal requirement • Dependent on the applicable legal instrument and purpose for processing • After the end of the prescribed period personal information is destroyed, anonymised or achieved	

#	Question	Response/Yes/No	Comment
	does the data processor have to give mirror access locally? • How long is the data stored? • Is the data destructed after that period of time, or kept? • Is that monitored independently, or only by the State?	• Monitored independently	
8	What does it imply in terms of data usage? • Can data be sold? • Can statistical data be sold? • Can technical data be sold?	• This has not been fully tested – but the implication is that data can be sold in compliance with privacy laws i.e full disclosures and express consent	
9	What control do people have on their data? • Are people informed of the	• Yes	

#	Question	Response/Yes/No	Comment
	data being collected? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) as a bulk? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) line by line? • How is that approval stored? • Who monitors it?	• Yes • No, people accept in bulk and not line by line • The Customer Permissions Management (CPM) system • Monitoring to be done by the business unit responsible for the CPM project	
10	Who is responsible for the implementation of the law? • NRA? • Ministry of ICT? • Army (or affiliate)? • Other?	• Information Regulator	

#	Question	Response/Yes/No	Comment
11	Who is responsible for possible breaches to the law? • Users? • Service provider? • Local operator? Just for themselves, or also on behalf of their counterparts? • Foreign operator / data handler?	• Responsible Party	
12	Implications of breach • Risks to companies – Penalties – Loss of license – Other • Risks to people – Penalties	Risk to companies • Financial penalties • Reputational damage Risks to people • Imprisonment	

#	Question	Response/Yes/No	Comment
	– Arrest – Other		
13	Who monitors the correct implementation of the law • Parliament? • Consumer associations / civil society? • Nobody? • Other?	• Information Regulator	

Country: Tanzania

Questionnaire

#	Question	Response/Yes/No	Comment
1	What is the relevant legislation? Are general data protection laws the only relevant laws or are there other sector specific laws as well that may impose additional requirements?	No	Tanzania does not have a specific law that governs data protection. However, there are other sector specific laws which provides for confidentiality and privacy. The following are laws governing data protection and privacy; • The Constitution of the United Republic of Tanzania, 1977 (Section 16(1)) • The Electronic and Postal Communications Act (EPOCA), 2010 (Sections 98, 99 and 120) • Regulation 6(2)(e) of the EPOCA (Consumer Protection) Regulations, 2018 • Regulation 4(1) of the EPOCA (Investigation) Regulations 2017 • The Cybercrimes Act, 2015 (Section 7) • Registration and Identification of Persons Act. R.E 2012 (Section 19)

#	Question	Response/Yes/No	Comment
			• Regulation 11 of EPOCA (Online Content) Regulations 2018 • The Records and Archives Management Act, 2002 (Section 16) • Access to Information Act, 2002 (Section 6(1) • The Statistics Act, 2015 (Section 25 (1)
2	Are there any bills currently before parliament, or expected to come before parliament, that propose to amend the existing regime?	No	There is no law governing data protection
3	What type of approach is this? • Consumer protection led? • Other?	No	There is no law governing data protection
4	What is the scope of the law? • Telecoms? • Social media? • Media? • Medical?	No	There is no law governing data protection

#	Question	Response/Yes/No	Comment
	• Banking? • Other?		
5	What does it imply in terms of data collection? • Do all types of data need to be captured, or only personal data? How are they categorised? • Is the data stored by the commercial entity or by a public entity? • Is the data copied / sent to a public entity?	No	There is no law governing data protection
6	What does it imply in terms of data storage? • Does data have to be stored locally? • Can data be stored outside of the country? • Can data stored locally be exported outside of the country? • Does that require an authorisation? • If so, by whom?	No	There is no law governing data protection
7	What does it imply in terms of data processing? • Do the same processes apply to all data, or only to personal data?	No	There is no law governing data protection

#	Question	Response/Yes/No	Comment
	• Are these processes same for technical and commercial usage? • Can data be processed abroad? If so, does the data processor have to give mirror access locally? • How long is the data stored? • Is the data destructed after that period of time, or kept? • Is that monitored independently, or only by the State?	No	There is no law governing data protection
8	What does it imply in terms of data usage? • Can data be sold? • Can statistical data be sold? • Can technical data be sold?	No	There is no law governing data protection
9	What control do people have on their data? • Are people informed of the data being collected? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) as a bulk?	No	There is no law governing data protection

#	Question	Response/Yes/No	Comment
	• Are people capable of accepting (= they want it) or rejecting (= they don't want it) line by line? • How is that approval stored? • Who monitors it?		
10	Who is responsible for the implementation of the law? • NRA? • Ministry of ICT? • Army (or affiliate)? • Other?	No	There is no law governing data protection
11	Who is responsible for possible breaches to the law? • Users? • Service provider? • Local operator? Just for themselves, or also on behalf of their counterparts? • Foreign operator / data handler?	No	There is no law governing data protection
12	Implications of breach	No	There is no law governing data protection

#	Question	Response/Yes/No	Comment
	• Risks to companies – Penalties – Loss of license – Other • Risks to people – Penalties – Arrest • Other		
13	Who monitors the correct implementation of the law • Parliament? • Consumer associations / civil society? • Nobody? • Other?	NO	There is no law governing data protection

Asia Pacific

Country: Australia

Questionnaire

#	Question	Response/Yes/No	Comment
1	What is the relevant legislation? Are general data protection laws the only relevant laws or are there other sector specific laws as well that may impose additional requirements?	The privacy law regime in Australia reflects Australia's federal system. The primary federal legislation is the *Privacy Act 1988* (Cth) (**Privacy Act**) which governs how personal information is handled in Australia in all industry sectors. It applies to all Australian Commonwealth Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses (collectively called **APP entities**). The 13 Australian Privacy Principles (**APPs**) form a part of this Act. Separate state and territory privacy laws apply to state and territory government agencies and contractors to those governments and their agencies. The state and territory privacy statutes typically include Information Privacy Principles (IPP) which are broadly similar to the federal APPs, with some differences. State based statutes: • **NSW**: Privacy and Personal Information Protection Act 1998 (NSW) and Health Records and Information Privacy Act 2002 (NSW) – regulates NSW public sector agencies and providers of health services. • **Victoria**: *Privacy and Data Protection Act 2014* (Vic) and *Health Records Act 2001* (Vic) - Victorian public sector agencies and providers of health services in Victoria and those providers' subcontractors. • **Queensland**: Information Privacy Act 2009 (Qld).	

#	Question	Response/Yes/No	Comment
		• **South Australia**: Department of the Premier and Cabinet Circular, PC012 – Information Privacy Principles Instruction, 16 September 2013. • **Tasmania**: Personal Information and Protection Act 2004 (Tas). • **Western Australia**: - no statutory regime however some privacy principles contained in the *FIO Act 1992* (WA). • **Australian Capital Territory**: I*nformation Privacy Act 2014* (ACT) and Health Records (Privacy and Access) Act 1997 (ACT). • **North Territory**: Information Act 2002 (NT). Sector based statutes: • **Healthcare sector:** – *My Health Records Act 2012* (Cth), *My Health Records Rule 2016* and *My Health Records Regulation 2012* – create a legislative framework for the Australian government's "My Health Record" system. *My Health Record Act 2012* (Cth) limits when and how health information included in a My Health Record can be collected, used and disclosed. – *Healthcare Identifiers Act 2010* (Cth), regulates (among other things) the use and disclosure of healthcare identifiers. – State and territory health information protection acts – *Health Records Act 2001* (VIC)*, Health Records (Privacy and Access) Act 1997* (ACT)*, Health Records and Information Privacy Act 2002* (NSW) – govern the handling of health information in both public and private sectors in these states and territories. This means private sector health providers in Vic, ACT and NSW must comply with both the federal and state/territory privacy legislation when handling health information. • **Telecommunications sector:** Part 13 of the *Telecommunications Act 1997* (Cth) imposes restrictions on the use and disclosure of telecommunications	

#	Question	Response/Yes/No	Comment
		and communications-related data. *Telecommunications (Interception and Access) Act 1979* (Cth) regulates the interception of and access to the content of communications transiting telecommunications networks and stored communications (eg SMS and emails) on carrier networks with enforcement agencies. This Act also includes requirements for mandatory retention of telecommunications metadata by carriage service providers to facilitate access to that information by law enforcement agencies. • **Finance sector:** Credit Reporting Systems (Part IIIA of Privacy Act), the CR Code and the Privacy Regulation 2013 regulate the handling of personal information about individuals' activities in relation to consumer credit. Also see regulations for Financial Service Providers Financial Service Providers (APRA Regulations CPS 231 and ASIC RG 104). Other statutes: • There is a range of other laws that impact privacy and data protection, both at federal and state/territory level. These include: – *Spam Act 2003* (Cth) (regulates sending of unsolicited electronic messages) and *Do Not Call Register Act 2006* (Cth) (regulates unsolicited commercial calling) – Laws governing the use of surveillance devices, tracking devices and listening devices, video and audio-visual monitoring of public places and workplaces, and computer and data surveillance of workplaces. See: ▪ Surveillance Devices Act 2016 (SA) ▪ *Listening Devices Act 1991 (TAS)* ▪ *Surveillance Devices Act 1999 (Vic)* ▪ *Surveillance Devices Act 1998 (WA)*	

#	Question	Response/Yes/No	Comment
		▪ *Surveillance Devices Act 2007 (NT)* ▪ *Surveillance Devices Act 2007* (NSW) ▪ *Listening Devices Act 1992 (ACT)* ▪ *Workplace Privacy Act 2011 (ACT)* ▪ *Workplace Surveillance Act 2005* (NSW) – *Data-matching Program (Assistance and Tax) Act 1990* (Cth) - regulates the federal government data-matching using tax file numbers. *Privacy (Tax File Number) Rule 2015* also regulates the collection, storage, use, disclosure, security and disposal of individuals' tax files numbers by public agencies and private organisations.	
2	Are there any bills currently before parliament, or expected to come before parliament, that propose to amend the existing regime?	In March 2019, the Government announced plans to amend the Privacy Act in relation to the enforcement regime. Some of the proposed reforms include: • An increase to the maximum penalty for serious and repeated interferences with privacy – up from $2.1m (for corporate entities) to the greater of $10m, 3 times the value of any benefit obtained through the misuse of the information and 10% of a company's annual domestic turnover; • Additional enforcement powers for the Office of the Australian Information Commissioner (**OAIC**) to issue infringement notices to companies and individuals for a failure to undertake remedial action to resolve minor privacy breaches. The maximum fines proposed are $63,000 for companies and $12,600 for individuals; • Greater enforcement and remedial powers for the OAIC, including the ability to publicise specific breaches and notify affected individuals and	

#	Question	Response/Yes/No	Comment
		• Specific rules to protect the personal information of children and other vulnerable groups. There is no draft legislation as yet and consultation for the proposed amendments is set to begin in the second half of 2019.	
3	What type of approach is this? • Consumer protection led? • Other?	• Consumer protection led: However, there is no general right to privacy in Australian law – either in the common law or the constitution. The relevant statutes create certain rights and protections for individuals which are directly enforceable by way of a largely complaints-based regime. • Other: Implementation of International Treaties Australia has acceded to, particularly for Cross Border Rules: – Detect and control transnational crime or conduct of criminal activities within Australia, including fraud, money laundering, tax evasion, modern slavery and exploitation of children and planning and funding terrorist activities. – Avoid adverse effects on national security interests.	
4	What is the scope of the law? • Telecoms? • Social media? • Media? • Medical? • Banking?	• The Commonwealth Privacy Act is general and applies to all private businesses (except small business) and Commonwealth Government agencies (APP entities). Each State has its own privacy law targeted at State agencies and healthcare. See above at item 1 ‘state based statutes’. • The Privacy Act has extra-territorial scope if an entity has an ‘Australian link’. An entity will have an Australian link where it conducts business in Australia (which may be made out even if an entity is not physically or legally established in Australia) and collects personal information in Australia. Personal information is collected ‘in Australia’ for the purpose of the Act if it is collected from an individual who is physically present in Australia or an external Territory regardless of where the collecting entity is located or incorporated.	

#	Question	Response/Yes/No	Comment
	• Other?	• There are specific requirements for certain industries – see the legislation listed above at item 1 'sector based statutes' and 'other statutes'.	
5	What does it imply in terms of data collection? • Do all types of data need to be captured, or only personal data? How are they categorised? • Is the data stored by the commercial entity or by a public entity? • Is the data copied / sent to a public entity?	• The Privacy Act applies to 'personal information' collected in Australia. Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable, (a) whether the information is true or not, and (b) whether the information is recorded in a material form or not. • Any handling of personal data, whether using, holding, processing or otherwise, is generally subject to the Privacy Act and the APPs. • Generally, consent is not required to collect personal information but the APPs provide, as a general rule, that an organisation should only use or disclose personal information for the purpose for which it was collected. However, an organisation may use or disclose personal information about a data subject for another purpose (a secondary purpose) if the data subject has consented or the secondary purpose is related to the primary purpose and such use or disclosure might reasonably be expected by the data subject. • There are stronger protections in the Privacy Act in relation to the collection of 'sensitive information'. This is information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, criminal record. In order to collect sensitive information, a data subject needs to have consented to such collection. Consent may be implied or expressed under the Privacy Act, but in any event requires both knowledge of the matter agreed to and voluntary agreement of the relevant data subject. The level of consent required in any particular case will depend upon, among other things, the seriousness of the consequences for the data subject if the personal data were to be used or disclosed.	

#	Question	Response/Yes/No	Comment
6	What does it imply in terms of data storage? • Does data have to be stored locally? • Can data be stored outside of the country? • Can data stored locally be exported outside of the country? • Does that require an authorisation? • If so, by whom?	• There are no general data localisation requirements in relation to personal information in Australia, however the following industry specific rules apply: – Telecommunications companies must provide an interception point in Australia. – Certain categories of government generated data are subject to rules precluding storage outside Australia. – Certain consumer credit information and limited categories of health information are precluded from being held outside Australia. • Before 'disclosing' personal information to an overseas recipient, APP 8.1 requires an APP entity to take reasonable steps to ensure that the overseas recipient does not breach the APPs except APP 1. This is known as the 'accountability principle': – There is a connected 'accountability liability' under s16C of the Privacy Act such that when an overseas entity operates in such a way that if they were an APP entity that they would have breached the APP principles then the disclosing APP entity is responsible. – There are exceptions to this requirement where (APP 8.2): ▪ the receiving entity is subject to a law or binding scheme with substantially similar protection and enforcement mechanism; ▪ individual consents to cross border disclosure after the entity informs them that APP 8.1 no longer applies if they give their consent; ▪ the disclosure is required or authorised by or under an Australian law or court order;	

#	Question	Response/Yes/No	Comment
		▪ the disclosure is in on of a limited number of "permitted general situations" such as to prevent or lessen a serious threat to life, health or safety; ▪ the entity is an agency and the disclosure of the information is required or authorised under an international agreement related to information sharing to which Australia is a party; or ▪ the entity is a government agency and the entity reasonably believes that the disclosure of the information is reasonably necessary for enforcement related activities conducted by or on behalf of an enforcement body. • **NB** There is a distinction between "use" and "disclose". There is no disclosure if the personal information remains at all times under the effective control of the APP entity. • There is no "general right to be forgotten". However, there is a limited indirect right to insist upon deletion or de-identification of personal information that an APP entity holds about an individual. APP 11.2 provides that if the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity and the information is not required by a law or court/tribunal order, the entity must take reasonable steps in the circumstances to destroy the information or to ensure that the information is de-identified.	
7	What does it imply in terms of data processing? • Do the same processes apply to all data, or only to personal data?	• The APPs provide that an APP entity may only hold, use or disclose personal information for the primary purpose for which it was collected and any other purpose that is related to the purpose for which the information was collected. • Each APP entity must have ongoing practices and policies in place to ensure that the entity manages personal information collected or held by it in an open and transparent way. APP entities must:	

#	Question	Response/Yes/No	Comment
	• Are these processes same for technical and commercial usage? • Can data be processed abroad? If so, does the data processor have to give mirror access locally? • How long is the data stored? • Is the data destructed after that period of time, or kept? • Is that monitored independently, or only by the State?	– Take reasonable steps to implement practices, procedures and systems that will ensure it complies with the APPs and is able to deal with related inquires and complaints – Have a clear and up to date privacy policy about how it manages personal information – Take reasonable steps to make its privacy policy available free of charge and in an appropriate form (usually on a website) • A privacy policy will need to include details as to: – Specific kinds of personal information that the entity collects and holds; – Purposes for which the entity collects, holds, uses and discloses personal information; – How an individual may access personal information about the individual that is held by the entity and seek the correction of such information; – How an individual may complain about a breach of the APPs; and – How the entity will deal with a complaint. • Consent is an exception to some APPs that prohibit personal information being handled in a particular way. Consent may be express or implied. An individual must be adequately informed before giving consent, give consent voluntarily, the consent must be current (not withdrawn) and the individual must have capacity to understand and communicate his/her consent.	

#	Question	Response/Yes/No	Comment
8	What does it imply in terms of data usage? • Can data be sold? • Can statistical data be sold? • Can technical data be sold?	The key activities regulated under Australian privacy law are collection, use and disclosure of personal information, including sensitive information. • **Collect** – an APP entity collects personal information only if the entity collects the personal information for inclusion in a print, electronic record or generally available publication. Collection may be manual or automated, entered by the affected individual or otherwise collected directly from that individual or obtained from a third party. • **Use** – generally, an APP entity uses personal information when it handles and manages that information within the entity's effective control. • **Disclose** – generally, an APP entity discloses personal information when it makes it accessible or visible to others outside the entity and releases the subsequent handling of the personal information from its effective control. • An entity that wishes to sell its personal information holdings can only do so if it has the consent of the individuals concerned before the sale is made. However, the sale of a whole business in respect of which customer information forms a part, for instance if the sale involves an asset sale, change of ownership or sale of shares of the business and personal information forms part of that business or assets, consent from data subjects may not necessarily be required.	
9	What control do people have on their data? • Are people informed of the data being collected? • Are people capable of accepting (= they	• An individual is conferred rights by the Privacy Act to: – Know who is collecting, using or disclosing information about them – Know why personal information is being collected, how it will be used or disclosed and who it will be disclosed to – Have the option of not identifying him-/herself or of using a pseudonym, in certain circumstances	

#	Question	Response/Yes/No	Comment
	want it) or rejecting (= they don't want it) as a bulk? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) line by line? • How is that approval stored? • Who monitors it?	– Ask for access to personal information about him-/herself – Stop receiving unwanted direct marketing – Ask for access to personal information that an APP entity holds about them and for any personal information that is incorrect to be corrected – Make a complaint about an APP entity, if the individual considers that it has mishandled personal information about him/her • There is no general right for an individual to object to collection, use or disclosure of personal information about that individual. The Act generally requires notice to individuals as to these activities and consent in relation to particular activities. • APP 2 provides that individuals must have the option of dealing anonymously or under a pseudonym with an APP entity. However, an APP entity does not have to provide this option where the entity is required by law to deal with identified individuals and/or it is impracticable for the entity to deal with individuals who have not identified themselves. • Individuals have a limited indirect right to insist upon deletion or de-identification of personal information that an APP entity holds about the individual. APP 11.2 provides that if the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity and the information is not required by a law or court/tribunal order, the entity must take reasonable steps in the circumstances to destroy the information or to ensure that the information is de-identified.	
10	Who is responsible for the implementation of the law?	• See below for at item 13 for Commissioners responsible for regulations and some enforcement. • APP 1 requires that entities take reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs. In this	

#	Question	Response/Yes/No	Comment
	• NRA? • Ministry of ICT? • Army (or affiliate)? • Other?	way, the APPs require 'privacy by design' – an approach where compliance is designed into projects dealing with personal information right from the start, rather than being dealt with afterwards. • Privacy Impact Assessments (PIAs) are commonly used as a means to assure privacy compliance.	
11	Who is responsible for possible breaches to the law? • Users? • Service provider? • Local operator? Just for themselves, or also on behalf of their counterparts? • Foreign operator / data handler?	• The Privacy Act provides several complaints paths for individuals where there has been a breach or alleged breach of an APP. The primary complaints process is through a complaint to the OAIC, initiating an investigation. This usually requires that the individual has first complained to the relevant APP entity. The OAIC has a range of regulatory powers it can then exercise in seeking various enforcement outcomes. **Data breach notifications scheme:** • If a relevant APP entity suspects there has been a data breach that is likely to result in serious harm to any of the affected individuals ("eligible data breach"), subject to some limited exceptions, it must: – Carry out a reasonable and expeditious assessment within 30 days of becoming aware as to whether there has been an eligible data breach; and – If an eligible data breach has occurred, notify the Information Commissioner and affected individuals as soon as practicable	
12	Implications of breach • Risks to companies – Penalties	• A breach of an APP in respect of personal information is an interference with the privacy of an individual. • There is no private right for an individual to claim damages for breach, only a right to enforce a declaration by the OAIC for compensation or to seek an injunction.	

#	Question	Response/Yes/No	Comment
	– Loss of license – Other • Risks to people – Penalties – Arrest – Other	• The OAIC powers include: – investigating complaints made in respect of alleged breaches of the Privacy Act or initiating its own investigations into suspected breaches; – seeking civil penalties against an organisation for serious or repeated interferences with the privacy of an individual (with penalties of up to $2.1 million for corporations); – accepting enforceable undertakings as to compliance with the Privacy Act; and – determining that an individual is entitled to loss or damage suffered as a result of a breach, including economic and non-economic loss – this may be determined following a complaint by a data subject or where the OAIC has initiated its own investigation (i.e. where no complaint has been made). • A civil penalty order financially penalises the relevant APP entity, but does not compensate individuals adversely affected by the contravention. Each civil penalty provision specifies a maximum penalty for contravention of that provision. • Civil penalty provisions in the Privacy Act include: – A serious or repeated interference with privacy (s 13G) – Various provisions set out in Part IIIA – Credit Reporting of the Privacy Act • An entity (or person) will contravene a civil penalty provision, and be liable to pay a penalty if it: – Attempts to contravene a civil penalty provision	

#	Question	Response/Yes/No	Comment
		– Aids, abets, counsels or procures contravention of a civil penalty provision – Induces a contravention of a civil penalty provision – Is knowingly concerned in or a party to a contravention of a civil penalty provision – Conspires with others to effect a contravention of a civil penalty provision (s 80V)	
13	Who monitors the correct implementation of the law • Parliament? • Consumer associations / civil society? • Nobody? • Other?	• **OAIC** – administers the Commonwealth Privacy Act. The OAIC is responsible for enforcing compliance with the Privacy Act and reviewing proposed privacy codes. • **State and territory Privacy, Information or Health Commissioners** - administer state and territory privacy statutes. These statutes apply to personal information held by respective state and territory government departments and agencies and contractors to them. – **NSW:** NSW Information and Privacy Commission. – **VIC:** Victorian Information Commissioner and Victorian Health Complaints Commissioner. – **NT:** Information Commissioner for the Northern Territory. – **ACT:** ACT Information Privacy Commissioner. – **WA:** Office of the Information Commissioner (WA). – **TAS:** Tasmanian Ombudsman. – **SA:** Privacy Committee of South Australia.	

#	Question	Response/Yes/No	Comment
		– **QLD:** Queensland Office of the Information Commissioner.	

Country: China

Questionnaire

#	Question	Response/Yes/No	Comment
1	What is the relevant legislation? Are general data protection laws the only relevant laws or are there other sector specific laws as well that may impose additional requirements?	**Legislation**[1] There is no overarching data protection law in China. However, important legislation containing data protection rules include the following: • The Tort Liability Law (2010) - expressly protects individual's right to privacy. • The Criminal Law, particularly the 7th (2009) and 9th (2015) Amendments – criminalises certain illegal sale, provision, stealing or acquisition of personal information. • The Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks (2012) - the first special legislation codifying personal information protection. • The General Provisions of the Civil Law (2017) – recognises an individual's rights over personal information as constituting fundamental civil rights. • The Cybersecurity Law (2017):[2] – The Cybersecurity Law is mainly devoted to safeguarding the "cyberspace sovereignty" of China and reinforcing	

[1] Dr Clarisse Girot, Regulation of Cross-Border Transfers of Personal Data In Asia, Asian Business Law Institute, 62 [1].

[2] Above n 1, 63 [2].

#	Question	Response/Yes/No	Comment
		cybersecurity. However, it also contains the most comprehensive and broadly applicable data privacy protection requirements to date in China. – Protection of personal information is a key element of the Cyber Security Law. The Law codifies the requirements embodied in existing laws and regulations, and incorporates new or more explicit requirements with respect to the right to correct and delete personal information, data breach notification, transfer of personal information, and data localisation. **Regulations/ Standards**[3] Important regulations and standards regarding data privacy protection or containing data privacy protection requirements include the following: • Guidelines for Personal Information Protection within Public and Commercial Services Information Systems (2013). • Provisions on Protecting the Personal Information of Telecommunications and Internet Users (2013). • Consumer Protection Law (2013 Revision). • Personal Information Security Specification ("PIS Specification").[4] – Ancillary regulation to the Cybersecurity Law. – Creates a comprehensive framework and imposes strict protection requirements throughout the data lifecycle.	

[3] Above n 1, 62 [1].

[4] Above n 1, 80 [25].

#	Question	Response/Yes/No	Comment
		– Considered the most important national standard in the implementation of data privacy protection requirements under Cybersecurity Law. – Voluntary standard, likely to serve as a referential basis for enforcement by regulatory authorities. **Sector-specific** There are a range of additional sector-specific data protection laws that apply to the following areas: • **Banking:** CBRC Circular on the Guidelines for Banking Consumer Protection (2013); CBRC Guidelines for the Regulation of Information Technology Outsourcing Risks of Banking Financial Institutions (2013); PBOC Circular on Doing a Good Job by Banking Financial Institutions in Protecting Personal Financial Information (2011); the PBOC Opinion on Further Strengthening the Info Security of Banking Financial Institutions (2006). • **Consumer Protection:** Protection of Consumer Rights and Interests Law (2014); Measures for Punishments against Infringements on Consumer Rights and Interests (2015), Measure on the Administration of Online Trading (2014). • **Credit Reporting:** Administrative Regulations on the Credit Reporting Industry (2013); Circular of the PBOC on Further Intensifying Management of Credit Information Security (2018); Administrative Measures for the Basic Databases of Personal Credit Information (2005); Circular on the Relevant Issues on Regulating Commercial Banks' Obtaining Authorisation to Inquire about Individual Credit Reports (2005). • **Healthcare:** Prevention and Treatment of Infectious Diseases Law (1989, 2013); Trial Measures for the Administration of Population	

#	Question	Response/Yes/No	Comment
		Health Information (2014); Administrative Provisions on the Medical Records of Medical Institutions (2014). • **Postal and Courier Services:** Security Measures on the Protection of Users' Personal Information for Mailing and Courier Services (2014). • **Telecommunications and Internet:** PRC Telecommunication Regulations (2000, 2016); Administrative Measures for the Protection of International Networking Security of Computer Information Networks (19997); Interim Provisions on the Administration of the Development of Instant Messaging Services (2014); Several Provisions on Regulating the Market Order for Internet Information Services (2013); Notice on Strengthening Administration over Network Access by Mobile Intelligent Terminals (2013), Provisions on Protection of Personal Information of Telecommunication and Internet Users (2013).	
2	Are there any bills currently before parliament, or expected to come before parliament, that propose to amend the existing regime?	There are no bills currently before parliament. However there are a number of proposed draft amendments to standards that currently regulate the protection of personal information. Most notably in early 2019, China's National Information Security Standardisation Technical Committee released draft amendments for comment in relation to the Personal Information Security Specification. The draft amendments propose to enhance the notice and consent requirements in relation to issues of forced or bundled consent and data over-collection, particularly in relation to access by third parties and targeted advertising.	

#	Question	Response/Yes/No	Comment
3	What type of approach is this? • Consumer protection led? • Other?	While protection of the rights of individuals is a prominent theme of the cross border data transfer rules, most laws and regulations are primarily driven by national security concerns.[5]	
4	What is the scope of the law? • Telecoms? • Social media? • Media? • Medical? • Banking? • Other?	As the cross-border data transfer rules mainly aim to protect national security, they are far-reaching and leave regulatory authorities plenty of room for discretion.[6] The majority of laws relate to foreign and domestic enterprises with business operations in China. Additionally, any organisation or individual would be subject to the law if they collect, process or use personal information of Chinese citizens within the territory of China, or if they transfer such data into or out of China. The law does not exempt any sector or institution from adherence to the requirements of due process in the performance of their respective offices, and no areas are beyond its scope. See response to question 1 for sector-specific laws.	
5	What does it imply in terms of data collection? • Do all types of data need to be captured, or only personal data? How are they categorised?	There are three types of data captured within existing legislation and regulations: • Personal Information; • Sensitive Personal Information; and • Important data.	

[5] Above n 1, 91 [45].

[6] Above n 1, 91 [46].

#	Question	Response/Yes/No	Comment
	• Is the data stored by the commercial entity or by a public entity? • Is the data copied / sent to a public entity?	**Personal information** • The Cybersecurity Law provides a unified definition for "personal information" under Chinese law (Article 76) for the first time.[7] • Cybersecurity Law defines personal information as "all kinds of information recorded in electronic or other forms, which can be used, independently or in combination with other information, to identify a natural person's personal identity", which "includes but is not limited to the natural person's name, date of birth, identity certificate number, biology-identified personal information, address and telephone number".[8] • Personal data is also defined under the PIS Specification using two criteria to define personal information.[9] • Information identifiable to a specific data subject; or • Information related to a specifically identified data subject. It provides a non-exhaustive list of personal information. **Sensitive personal information** • The PIS Specification provides a broad definition of sensitive personal information, which is defined as any personal information that would endanger the personal or property safety, cause harm to the reputation or physical or mental health, or lead to discriminatory treatment of data subjects.[10]	

[7] Above n 1, 75 [20].
[8] Above n 1, 76 [20].
[9] Above n 1, 81 [25].
[10] Above n 1, 81 [25].

#	Question	Response/Yes/No	Comment
		• Incudes information commonly processed by financial institutions, such as phone numbers, account numbers, transaction records, credit records, deposit information and virtual currencies of data subjects. **Important data** • First introduced into law by the Cybersecurity Law but was left undefined (Article 31).[11] • The Cybersecurity Administration of China (**CAC**) has formulated draft guidelines which enumerates important data across industries. • The Draft Data Export Guidelines enumerates important data in 28 industries and sectors, such as the resources and energy, telecommunications and electronic manufacturing industries. Data generally can be stored by any entity, so long as there is a lawful basis for its collection and processing. It does not require the data to be sent or stored by a third party.	
6	What does it imply in terms of data storage? • Does data have to be stored locally? • Can data be stored outside of the country?	**Data storage in the Cybersecurity Law**[12] • The Cybersecurity Law explicitly provides data localisation requirements at the level of national laws in China, which are only applicable to critical information infrastructure operators (**CIIOs**). • CIIOs are required to store data domestically within China, and may only transfer such information and data abroad due to business needs, with prior consent from the data subject, completion of a	• Critical information infrastructure operators (**CIIOs**) CIIOs are 'network operators', that is, "owners and administrators of networks and network services" (Article 76) subject to heightened

[11] Above n 1, 76 [20].
[12] Above n 1, 74 [20].

#	Question	Response/Yes/No	Comment
	• Can data stored locally be exported outside of the country? • Does that require an authorisation? • If so, by whom?	security assessment and approval from competent industry authorities. **Data storage before Cybersecurity Law** Before the adoption of the Cybersecurity Law, regulations governing cross-border transfer of data from China were interspersed across a number of sectoral laws and regulations governing specific industries or types of data.[13] *State secrets* • Without approval by competent departments, no document or other material or objects classified as a state secret or information containing state secrets may be carried, transmitted, posted or transferred out of China (Cybersecurity law).[14] *Financial regulations* • The Notice of the People's Bank of China on Urging Banking Financial Institutions to Strengthen the Protection of Personal Financial Information ("2011 PBOC Notice") issued by the People's Bank of China ("PBOC") in 2011 requires banks to process personal financial information collected in China locally and not to transfer such information overseas.[15] • Measures of the People's Bank of China for Protecting Financial Consumers' Rights and Interests22 issued by PBOC in 2016	cybersecurity requirements under Cybersecurity Law.[24] • Critical information structures are information infrastructures in "public communication and information services, energy, traffic and transportation, irrigation, finance, public service, e-government, and other key industries and sectors", as well as other information infrastructures, "the damage, malfunction and data leakage of which may seriously endanger national security, national welfare, people's livelihood and public interest' (Article 31).[25] *State secrets*[26]

[13] Above n 1, 65 [5].
[14] Above n 1, 67 [8].
[15] Above n 1, 67 [9].
[24] Above n 1, 74 [20].
[25] Above n 1, 75 [20].
[26] Above n 1, 66 [7].

#	Question	Response/Yes/No	Comment
		provides exceptions to this rule for transferring such information abroad, including situations where: – the transfer has been authorised by the data subject; – the information is transferred to the bank's overseas affiliates such as the head office, parent company or branch companies, subsidiaries or other affiliated institutions required for completing the business; and – the transferring party shall require the receiving party to effectively protect information through contracts and conducting on-site inspection.[16] • Regulation on Administration of Credit Investigation Industries (2015) 23 and the Decision of the State Council on Implementing Access Administration of Bank Card Clearing Institutions (2015) provides credit reporting agencies are to store and process information collected within China. Bank card clearing institutions are required to deploy infrastructure capable of completing bank card clearing business independently and remote disaster system within China, and use such domestic infrastructure to process domestic bank card clearing business.[17] *Human genetic resources* • According to the HGR Interim Measures, any export of human genetic resources from China is to be approved by the Ministry of Sciences and Technology.[18]	• State secrets are very broadly defined under the State Secret Laws. • In general, any non-public information or matter that has a vital bearing on state security and national interests may be classified as a state secret and be subject to confidentiality measures. • Information relating to national security, military and foreign affairs, national economy, science and technology development and other strategic matters of the state constitutes a state secret if its disclosure may be deemed to harm national security and interests in the areas of politics, economy, national defence or foreign relations. • The scope of state secrets is to be determined by the

[16] Above n 1, 68 [9].
[17] Above n 1, 69 [9].
[18] Above n 1, 69 [11].

#	Question	Response/Yes/No	Comment
		• Exceptions: any form of cross border-movement of Chinese human genetic resources cannot be done without prior approval from the Government; and parties must obtain informed consent of the data subject in writing for the transfer of their human genetic resources.[19] *Demographic health information* • The Interim Measures for the Administration of Demographic Health Information (2014) ("DHI Interim Measures")29 issued by the National Health and Family Planning Commission prohibits medical institutions from storing demographic health information in any server outside China as well as the hosting or leasing of any server outside China for the processing of demographic health information.[20] *Location and mapping data* • Some location and mapping data may constitute state secrets in surveying and mapping areas and will thus be subject to the regulations safeguarding state secrets. For instance, co-ordinates with a particular level of precision or coordinates of certain key facilities are classified as state secrets under the Measures on the Scope of State Secrets in the Administration of Survey and Mapping (2002) and its attachment Catalogue of State Secrets in the Administration of Survey and Mapping, and are therefore prohibited from being stored and transferred out of China.[21] • The regulations on map services, ie, the Regulations on Map Administration (2015), imposes data localisation requirements on	• State Secrets Bureau in conjunction with other relevant government departments responsible for the protection of state secrets within their respective jurisdictions and may be adjusted by such government agencies from time to time. *Human genetic resources*[27] • Human genetic resources are defined as "resources and materials, such as human organs, tissues, cells, nucleic acid and nucleic acid products which contain human genome, genes or gene products, as well as any information derived from such resources and materials". *Demographic health information*[28] • Includes both individual personal health data as

[19] Above n 1, 70 [12].
[20] Above n 1, 71 [13].
[21] Above n 1, 71 [14].
[27] Above n 1, 69 [11].
[28] Above n 1, 71 [13].

#	Question	Response/Yes/No	Comment
		map data even if the data do not constitute state secrets. Pursuant to these regulations, Internet map service providers are required to store map data in servers in China and implement the corresponding data security protection systems.[22] *Internet regulations* • The Provisions on the Administration of Online Publishing Services (2015), the Interim Measures for the Administration of Online Taxi Booking Business Operations and Services (2016), and the Draft of Notice on Regulating Business Operation in Cloud Service Market (2016), require the servers and data storage of these service providers to be hosted within China.[23]	well as aggregated population health data.
7	What does it imply in terms of data processing? • Do the same processes apply to all data, or only to personal data? • Are these processes same for technical and commercial usage? • Can data be processed abroad? If so, does the data processor have to give mirror access locally?	The Cybersecurity Law is promulgates that there must be a lawful basis for processing (ie, not forced or fraudulent) and that there must be a necessary and clear purpose for the processing. This applies generally to data, however there are certain rights applicable in relation to personal data. For example, an individual can object to the processing of their data. Additionally, an individual's consent is a prerequisite for cross-border data transfer. There are some types of data that are subject to more stringent processing rules: • **Personal financial information**: This must be stored, processed and analysed within China. No transfers overseas are permitted unless otherwise authorised. • **Personal credit information**: The assembly, storage and processing of information collected by a credit reporting entity from	

[22] Above n 1, 71 [14].

[23] Above n 1, 72 [15].

#	Question	Response/Yes/No	Comment
	• How long is the data stored? • Is the data destructed after that period of time, or kept? • Is that monitored independently, or only by the State?	within the territory of China must also be carried out within the territory of China. Throughout the storage term, each entity must maintain a record of its employees' access to such information. • **Personal health information**: This information may not be stored in overseas servers (including servers hosted in and leased from foreign countries). Generally, circumstances surrounding the transfer of personal information to outsourced processing services vary, depending on the industry. Industrial regulators may provide general and specific relevant guidance. The Data Protection Guidelines and Personal Information Security Specifications provide relevant non-binding, recommended best practices and managerial and technical standards. For example, before data is processed by a third party, the primary data controller should conduct a security impact assessment to ensure that such data processor has the necessary data security capability.	
8	What does it imply in terms of data usage? • Can data be sold? • Can statistical data be sold? • Can technical data be sold?	Data may only be sold if the data subject has consented to such sale. Otherwise, it is illegal to sell data, as network service providers and other enterprises, public institutions and their employees are obligated to strictly keep confidential electronic information collected during their business activities and may not disclose, falsify, damage, sell or illegally provide such information to others.	

#	Question	Response/Yes/No	Comment
9	What control do people have on their data? • Are people informed of the data being collected? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) as a bulk? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) line by line? • How is that approval stored? • Who monitors it?	The law does not establish any general obligation to provide notice to, or consult with, an individual with respect to collected personal information. The Data Protection Guidelines propose that a consent notice to a prospective individual should encompass a range of information relating to the collection method, retention period, scope of use, compliance procedures and anticipated transfers to third parties.	
10	Who is responsible for the implementation of the law? • NRA? • Ministry of ICT? • Army (or affiliate)?	There is no singly regulatory authority that exercises sole responsibility for the oversight of China's data protection law. It is generally divided into criminal and administrative components. **Criminal:** the Ministry of Public Security is the primary law enforcement agency. **Administrative:**	

#	Question	Response/Yes/No	Comment
	• Other?	• Cybersecurity administration of China (CAC) is the major implementing authority of the Cybersecurity Law.[29] • Industrial regulatory authorities (for example, the China Banking and Insurance Regulatory Commission, or the State Market Regulatory Administration. • The National Information Security Standardization Technical Committee ("TC 260").	
11	Who is responsible for possible breaches to the law? • Users? • Service provider? • Local operator? Just for themselves, or also on behalf of their counterparts? • Foreign operator / data handler?	The laws generally state that 'network operators' and CIIOs are deemed the responsible party if there was a breach. **Network operators** • "Network operators" are defined as "owners and administrators of networks and network service providers" (Article 76).[30] • Considered a sweeping definition not only cover providers of telecommunication or Internet services but may also encompass any public or private entities that own or operate IT networks for internal usage.[31] **CIIOs** • CIIOs are a subset of network operators subject to heightened cybersecurity requirements under the Cybersecurity Law.[32] • Critical information infrastructures are information infrastructures in "public communication and information services, energy, traffic and	

[29] Above n 1, 76 [23].
[30] Above n 1, 76 [20].
[31] Above n 1, 76 [20].
[32] Above n 1, 76 [20].

#	Question	Response/Yes/No	Comment
		transportation, irrigation, finance, public service, e-government and other key industries and sectors", as well as other information infrastructures, "the damage, malfunction and data leakage of which may seriously endanger national security, national welfare, people's livelihood, and public interest" (Article 31).[33]	
12	Implications of breach • Risks to companies – Penalties – Loss of license – Other • Risks to people – Penalties – Arrest – Other	Companies generally face financial penalties for non-compliance with the Cybersecurity Law. CIIOs violating data localisation requirements could trigger a wide range of potential penalties including: • warnings; • suspensions of operation; • the revoking of business licences and permits; and • fines up to RMB500,000.[34]	
13	Who monitors the correct implementation of the law • Parliament?	The Cyberspace Administration of China is responsible for supervising the implementation of the law generally, while the Ministry of Industry and Information Technology, the public security department and other relevant departments are responsible for the supervision and administration of personal information protection in their respective sectors.	

[33] Above n 1, 77 [20].
[34] Above n 1, 76 [22].

#	Question	Response/Yes/No	Comment
	• Consumer associations / civil society? • Nobody? • Other?		

Country: India

Questionnaire

#	Question	Response/Yes/No	Comment
1	What is the relevant legislation? Are general data protection laws the only relevant laws or are there other sector specific laws as well that may impose additional requirements?	India does not currently have any specific data protection legislation.[35] However it does have legislation and policies which partially address data protection. The current laws and policies in place include general law (IT Act, IT Rules) as well as sectoral law (Unified Access Services Licence, Unified License – telecommunications) **Legislation** The *Information Technology Act* (**IT Act**) states that where a body corporate possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.[36] The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (**IT Rules**) state that "sensitive personal data or information" may be disclosed (within or outside India) only if the disclosure is necessary for the performance of the contract with	The most relevant legislation is section 43A of the IT Act and the accompanying Section 43A Rules. There is also a collection of sectoral laws and policies (for example telecommunications). Aadhaar is a 12-digit unique identity number issued by UIDAI (an agency of India's IT Ministry) to Indian residents.

[35] Dr Clarisse Girot, Regulation of Cross-Border Transfers of Personal Data In Asia, Asian Business Law Institute, 117 [1].

[36] Above n 1, 122 [17].

#	Question	Response/Yes/No	Comment
		the provider of information, or where the provider has consented to the transfer[37] (which also applies to third-party processors). The Unified Access Services Licence (**UASL**) and the Unified License (**UL**) (two sets of regulations under the Department of Telecommunications) state: The Licensee shall not transfer the following to any person/place outside India: • Any accounting information relating to subscriber (except for international roaming/billing) (Note: it does not restrict a statutorily required disclosure of financial nature); • User information (except pertaining to foreign subscribers using Indian Operator's network while roaming and IPLC subscribers)…[38] The Companies (Accounts) Rules, Ministry of Corporate Affairs, 2014 (**CAR**) mandates there should be a back-up of financial information and other books/papers of the company stored periodically within Indian borders.[39] Aadhar Regulations (Data Security and Sharing of Information), Unique Identification Authority of India (**UIDAI**), 2016.[40] **Policy** National Data Sharing and Accessibility Policy (**NDSAP**) Department of Science and Technology (**DST**), 2012 advocates	

[37] Above n 1, 122 [19].
[38] Above n 1, 123 [21].
[39] Above n 1, 129 [38].
[40] Above n 1, 130 [38].

#	Question	Response/Yes/No	Comment
		for government-processed data to be stored in data centres within Indian borders.[41] The Guidelines for Government Departments on Contractual Terms Related to Cloud Services (**Cloud Services Guidelines**), MeitY, 2015 state that cloud service providers wanting government contracts/funds must store data physically in India.[42]	
2	Are there any bills currently before parliament, or expected to come before parliament, that propose to amend the existing regime?	In August 2017, the Ministry of Electronics and Information Technology, Government of India (**MeitY**) constituted a Committee of Experts on a Data Protection Framework for India (**Srikrishna Committee**) for the purpose of investigating data protection issues and suggesting a draft Data Protection Bill.[43] The Srikrishna Committee published a white paper in December 2017 on the proposed data protection framework and invited comments from the public. Based on the comments, public consultations and internal deliberations, the Srikrishna Committee submitted its final report and a draft bill to the MeitY on 27 July 2018. As a result, the government of India issued a draft Personal Data Protection Bill, 2018 (**Draft Bill**) in November 2018. However, it is likely that it will not be tabled in Parliament until June 2019. **Draft Bill summary** **Application**	

[41] Above n 1, 129 [38].
[42] Above n 1, 129-30 [38].
[43] Above n 1, 120 [10].

#	Question	Response/Yes/No	Comment
		Applies to personal data processed in India and persons who are based in India. Will also apply to processing of personal data in connection with business carried on in India. Encapsulates personal data, sensitive personal data and critical personal data. **Processing** Processing of personal data can only be in relation to fair and reasonable processing with a limited purpose, and can only be processed in connection with the purpose for which it was collected. The individual should be given notice at the time the data is collected and the data should not be inaccurate. Personal data can only be stored for as long as reasonably necessary to satisfy the processing purpose (unless other retention periods apply). There is a generally stricter approach taken to sensitive personal data (eg, consent for collection must be explicit consent; necessary processing offshore must be strictly necessary). There are a range of limited exemptions relating to the application of the processing requirements in Draft Bill. These include: (i) interest of security of the State, (ii) interest of law enforcement, (iii) disclosure in legal proceedings, (iv) research, archiving or statistical purposes, (v) personal and journalistic purposes, and (vi) processing by small entities. **Individual rights** Individuals have a range of rights in relation to their personal data. These include (i) right to correction, (ii) right to confirmation of processing, (iii) right to access data, (iv) right to be forgotten,	

#	Question	Response/Yes/No	Comment
		and (v) right to require data to be provided in a structured, commonly used and machine readable format. **Accountability** Collecting entities must have data fiduciaries, who are responsible for complying with all obligations set out in the Draft Bill. This includes ensuring that applicable data processors comply with their obligations. **Data breaches** Data breaches must be notified to the Data Protection Authority (**DPA**) if the breach is likely to cause harm to the individual. The DPA may then request that the individual also be notified. **Storage + transfer** Personal data and sensitive personal data must have at least one copy stored in India. Critical data can only be processed in India. Personal data may be transferred outside of India with individual consent. Critical personal data can only be transferred out of India if it relates to strictly necessary action in relation to health or emergency services. **Penalties** Monetary penalties can be up to 2-4% of worldwide company turnover. Criminal sanctions apply and are non-bailable – including imprisonment for up to 3 years. Affected individuals can also seek compensation.	

#	Question	Response/Yes/No	Comment
3	What type of approach is this? • Consumer protection led? • Other?	**Current legislation/policy** Data localisation laws and policies are designed to protect users from data/privacy loss.[44] With regards to the telecommunications industry and data collected by government agencies (eg UIDAI), there is also an emphasis on preserving national security and citizens' privacy.[45] **Pending legislation/policy** The push for the Draft Bill has been driven by citizen protection, consumer protection and IT industry growth concerns.[46] The *Puttaswamy v Union of India* ("*Puttaswamy*") judgment read privacy into fundamental rights and the Indian Constitution.[47] As such, the Indian government is concerned to protect the constitutionality of current laws by legislating comprehensively to protect data.[48] The Srikrishna Committee released a White Paper which recognised that stronger legislation on cross-border data transfers is needed for small and medium-sized enterprises, consumers and multi-national businesses, as well as being critical to the "digital economy".[49]	

[44] Above n 1, 129 [37].
[45] Above n 1, 131 [49].
[46] Above n 1, 117 [1].
[47] Above n 1, 117 [3].
[48] Above n 1, 118 [5].
[49] Above n 1, 121 [14].

#	Question	Response/Yes/No	Comment
4	What is the scope of the law? • Telecoms? • Social media? • Media? • Medical? • Banking? • Other?	The scope of the IT Act is very broad. It covers sensitive personal data owned or used by body corporates.[50] "Body corporate" is defined broadly[51] and doesn't distinguish between controllers, processors or intermediaries.[52] "Sensitive personal data" includes a person's password; financial information; physical/physiological/mental health information; medical information; and more.[53] The UASL and UL covers telecommunications specifically, and applies to all customer accounting and user information (other than roaming information).[54]	The law covers body corporates, with specific data localisation laws/policies for the telecommunications sector
5	What does it imply in terms of data collection? • Do all types of data need to be captured, or only personal data? How are they categorised? • Is the data stored by the commercial entity or by a public entity?	The IT Act covers sensitive personal data and provides for compensation to people who suffer as a result of a company negligently implementing and maintaining security practices. This implies that data is stored by the commercial entity (the company) and they are responsible for its protection. The data localisation laws mainly encompass data collected from local citizens when using applications and other related technology[55] – as such, all data appears to be captured. Some policies (such as NDSAP and Cloud Services Guidelines) impose requirements for government-held/processed data. Others (such as the Companies (Accounts) Rules) impose requirements on private companies. Therefore, there is no	Section 43A/Rule 7 only covers sensitive personal data, and suggests data can be collected by a body corporate within or outside of India via authorised transfer (the data "importer"). No mention of a public entity is made. Data localisation laws/policies generally cover any data collected from citizens, although: • the Companies (Accounts) Rules only apply to financial

[50] Above n 1, 133 [55].
[51] Above n 1, 134 [57].
[52] Above n 1, 133 [56].
[53] Above n 1, 134 [61].
[54] Above n 1, 133 [54].
[55] Above n 1, 131 [47].

#	Question	Response/Yes/No	Comment
	• Is the data copied / sent to a public entity?	central data collection entity (public or commercial) being governed by Indian data protection laws, rather laws that apply to data collected by private and public entities. However, the data collected by government agency Aadhar is stored in fully secured servers in its own data centre (located within India).[56]	information/other books or papers of the company; • UASL and UL cover user financial and accounting information. Data can be either collected by the commercial entity (through e.g. when citizens use apps), or by a public agency (e.g. UIDAI for the Aadhaar initiative). Data collected by commercial entities does not appear to be sent to a public entity. A proposed policy is the *National Telecom M2M Roadmap*, which states "all gateways and application servers serving customers in India **and in turn, collecting information**, must store it within the country." The Draft Bill contemplates application to personal data, sensitive personal data and critical personal data. Each type of data is treated differently with respect to collection and processing.
6	What does it imply in terms of data storage? • Does data have to be stored locally?	Data localisation laws require that data be stored within India. The UASL and UL, NDSAP, CAR, and Cloud Services Guidelines all mandate that data be stored within India.[57]	Data is generally required to be stored locally (or at least backed up locally). Data can be exported outside of the country, however it must comply with

[56] Above n 1, 132 [50].

[57] Above n 1, 129-130 [38], 133 [54]. NDSAP (government-processed data); CAR (backups of financial information); Cloud Services Guidelines (data from government contracts/public funds).

#	Question	Response/Yes/No	Comment
	• Can data be stored outside of the country? • Can data stored locally be exported outside of the country? • Does that require an authorisation? • If so, by whom?	Data collected by government agency Aadhar is stored in secure servers within India, and the UIDAI has stated that data cannot be accessed by the outside world.[58] The IT Rules prescribe that data transfer abroad (by body corporates) is allowed if the same level of data protection is observed in the country of destination; if it is necessary for the performance of the contract; and if the person has consented to the transfer.[59] Under telecommunications laws (UASL and UL) remote access to customer accounting and user information (aside from roaming information) from outside India is prohibited.[60]	certain requirements stipulated in Section 43A and Rule 7. The Draft Bill anticipates varying storage and transfer rules based on the type of data collected. Personal data and sensitive personal data must have at least one copy stored in India, whereas critical data can *only* be processed in India. Personal data may be transferred outside of India with individual consent. Critical personal data can only be transferred out of India if it relates to strictly necessary action in relation to health or emergency services.
7	What does it imply in terms of data processing? • Do the same processes apply to all data, or only to personal data? • Are these processes same for technical and commercial usage?	The IT Rules only apply to sensitive personal data or information and not all personal data.[61] The consent obligations contained these rules with respect to data processing practices by body corporates of sensitive personal data do not contain an onshore data storage restriction.[62] Data collected by UIDAI is processed within India and is not accessible outside of India.[63] Neither the IT Act nor the IT Rules provide specific timeframes for retention of sensitive personal information. However, they do not override other laws that may specify maximum periods of	There are not uniform data processes applied to data generated within India. Data is generally processed within India (eg Aadhaar initiative data), although Section 43A/Rule 7 does not have an onshore data storage restriction in its consent obligations. The Draft Bill anticipates a higher level of processing standard in relation to sensitive personal data. For example, the processing of personal data only requires notification

[58]

[59] Above n 1, 136 [69].

[60] Above n 1, 133 [54].

[61] Above n 1, 135 [61].

[62] Above n 1, 136 [68].

[63] Above n 1, 132 [50].

#	Question	Response/Yes/No	Comment
	• Can data be processed abroad? If so, does the data processor have to give mirror access locally? • How long is the data stored? • Is the data destructed after that period of time, or kept? • Is that monitored independently, or only by the State?	retention for sensitive data. For example, telecom licenses require licensees to maintain all commercial records for at least one year.	and consent. However, the processing of sensitive personal data requires explicit consent that is deemed satisfied through a range of criteria. Data can only be stored for as long as reasonably necessary to satisfy the processing purpose, unless other retention periods apply under other legislation.
8	What does it imply in terms of data usage? • Can data be sold? • Can statistical data be sold? • Can technical data be sold?	There is nothing that explicitly states that data cannot be sold, however this is subject to the general disclosure obligation to have prior consent of the data subject before data can be disclosed to third parties.	

#	Question	Response/Yes/No	Comment
9	What control do people have on their data? • Are people informed of the data being collected? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) as a bulk? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) line by line? • How is that approval stored? • Who monitors it?	When collecting sensitive personal data, the data subject must be made aware through reasonable steps of the fact that information is being collected, the purpose for which it is collected, the intended recipients of the information and the name and address of the agency collecting or retaining the information. Consent must be obtained from the data subject regarding purpose of usage before collection of the information. There are various other rights that individuals have in relation to control of their data. This includes rights to: • access their data; • rectification of errors; • request deletion; • object to, or restrict, processing; • control disclosure; and • restrict marketing.	ɾ the Draft Bill, individuals will have a range of rights in relation to their personal data. These include (i) right to correction, (ii) right to confirmation of processing, (iii) right to access data, (iv) right to be forgotten, and (v) right to require data to be provided in a structured, commonly used and machine readable format.
10	Who is responsible for the implementation of the law? • NRA? • Ministry of ICT? • Army (or affiliate)?	There is no specific data protection authority in India. The law is implemented principally through the MeitY. However, given that much of India's data protection legislation has been created on a sectoral basis, a number of government department/agencies are responsible for implementing sector-specific legislation/policy. Other departments/agencies include:	The Ministry of Communications and Information Technology was bifurcated into (1) the Ministry of Communications, and (2) the MeitY, in 2016. Under the Draft Bill, it is anticipated that the Data Protection Authority will be the primary supervisory authority of the law.

#	Question	Response/Yes/No	Comment
	• Other?	• The Department of Science and Technology (created the NDSAP); • The Ministry of Corporate Affairs (created the CAR); • The Department of Telecommunications (created the UASL and UL).	
11	Who is responsible for possible breaches to the law? • Users? • Service provider? • Local operator? Just for themselves, or also on behalf of their counterparts? • Foreign operator / data handler?	The IT Act states that body corporates who fail to properly implement security practices will be liable to pay damages to any person affected. As such, the onus falls on the company transferring data to maintain sufficient security practices. UIDAI has made public statements guaranteeing that data collected for the Aadhaar initiative is not accessible outside India,[64] suggesting that it is responsible for the implementation of the Aadhar Regulations (and thus possible breaches).	Under the Draft Bill, collecting entities must have appointed data fiduciaries, who are responsible for complying with all obligations set out in the Draft Bill. This includes ensuring that applicable data processors comply with their obligations.
12	Implications of breach • Risks to companies – Penalties	Body corporates who breach their obligations risk having to pay damages to people negatively impacted by their actions.[65] This also applies to persons acting on the body corporate's behalf.[66] The law does not prescribe a maximum compensation, however can include fines and imprisonment.	Under the Draft Bill, consequences of breaches can include: Monetary penalties: up to 2-4% of worldwide company turnover.

[64] Above n 1, 132 [50].
[65] Above n 1, 122 [17].
[66] Above n 1, 133 [55].

#	Question	Response/Yes/No	Comment
	– Loss of license – Other • Risks to people – Penalties – Arrest – Other		Criminal sanctions: including non-bailable offences and imprisonment for up to 3 years. Compensation: affected individuals can also seek compensation.
13	Who monitors the correct implementation of the law • Parliament? • Consumer associations / civil society? • Nobody? • Other?	There are no specific national bodies that deal with the implementation and administration of the law.	The White Paper envisions a separate and independent data protection authority for monitoring and enforcement of a data protection legal framework.[67] However, this is not yet the law.

[67] Above n 1, 140 [83].

Country: Indonesia

Questionnaire

#	Question	Response/Yes/No	Comment
1	What is the relevant legislation? Are general data protection laws the only relevant laws or are there other sector specific laws as well that may impose additional requirements?	There is no consolidated data protection law in Indonesia. However, there are a number of laws that address data protection issues. The key laws and regulations are Law No. 11 of 2008 on Electronic Information and Transaction, as amended by Law No. 19 of 2016 (**EIT Law**) and its implementing regulations: (i) Government Regulation No. 82 of 2012 on Implementation of Electronic Systems and Transactions (**GR 82/2012**); and (ii) Menkominfo Regulation No. 20 of 2016 on Protection of Personal Data in Electronic Systems (**MCI Regulation 20/2016**), (together, the **Data Protection Laws**). **Legislation** • EIT Law: • Article 26 requires consent to be given before personal data can be used through electronic media. • Article 26 was also amended to include a right of individuals to request deletion of their personal data. • Article 1(1) prohibits transferring electronic information or documents (including stored data) to an unauthorised party. **Regulations** • Article 15(1)(c) of GR 82/2012 requires system providers to gain consent for the collection, use and disclosure of personal data from the	MCI Regulation 20/2016 defines personal data as any true and actual information that adheres and can be identified, either directly or indirectly, to an individual, which is used in accordance with the laws and regulations, that is stored and maintained, the truthfulness of which is maintained and the secrecy of which is protected.

#	Question	Response/Yes/No	Comment
		data subject. Data may only be disclosed to a third party if the disclosure aligns with the original purpose for which it was collected.[68] • MCI Regulation 20/2016 Articles 21 and 22 require consent to be gained for data transfers and that cross-border transfers of personal data must be co-ordinated with the MCI. This regulation applies to both local and foreign electronic system providers (**ESPs**). • MCI Regulation 20/2016 requires all ESPs to store personal data in encrypted form. • Article 28(a) of MCI Regulation 20/2016 requires the data processing system to be certified. This will not apply however, until the certification of electronic systems regulation is implemented. • Article 6 and Article 1(4) of the MCI Regulation 20/2016 require an individual's consent for any transfer of personal data to a third party. **Constitutional Protections** • The Indonesian Constitutional Court has found an implied right to privacy in Article 28G of the 145 Constitution of the Republic of Indonesia.[69] **International Commitments** • Indonesia has ratified the International Covenant on Civil and Political Rights (**ICCPR**). Indonesia have also signed the Optional Protocol and Second Optional Protocol to the ICCPR. • The Association of Southeast Asian Nations (ASEAN) Economic Community (AEC) has signed FTAs with other Asian countries	

[68] Dr Clarisse Girot, Regulation of Cross-Border Transfers of Personal Data In Asia, Asian Business Law Institute, 143 [3].

[69] Above n 1, 145 [10].

#	Question	Response/Yes/No	Comment
		containing data protection clauses. As an ASEAN Member State, Indonesia is bound by these clauses. • Indonesia has committed to the Master Plan on ASEAN Connectivity (**MPAC**) which is an initiative to implement a digital data governance framework that covers privacy protection between 2018-2025. **Data protection regulations in the financial sector** • Article 31 of the Financial Services Authority Regulation Number 01/POJK.07/2013 provides that a financial service institution is not allowed to make local or international transfer of consumer data unless the consumer has consented in writing or it is required by law. The Indonesian Financial Services Authority (**OJK**) can impose sanctions for non-compliance with these regulations.[70] • Article 50 of the Financial Services Authority Regulations POJK 69/2016 requires: – insurance and reinsurance companies to collect data beyond just personal data, including data from payment transactions and claims, population data and administrative data; and – all banks, insurers and reinsurers to locate their data centres in Indonesia. • Bank Indonesia's Regulation No. 9/15/PBI/2007 on the Implementation of Risk Management in the Utilisation of Information Technology by the Bank stipulates that the bank's customer data transfer (by way of establishing a data centre or data processing outside the Indonesia	

[70] Above n 1, 148 [19-20].

#	Question	Response/Yes/No	Comment
		territory) necessitates prior approval being obtained from Bank Indonesia. **Other specific laws** • Article 40 of Law 36/1999 provides that any person is prohibited from any kind of tapping of information transmitted through any kind of telecommunications network. Article 42 stipulates that any telecommunications services operator has to keep confidential any information transmitted or received by a telecommunications service subscriber through telecommunications networks or telecommunications services provided by the relevant operator. • Article 6 of Law 14/2008 regarding Disclosure of Public Information provides that information relating to personal rights may not be disclosed by public bodies. Article 17 of the relevant law, together with other laws, prohibits the disclosure of private information of any person, particularly that which concerns family history; medical and psychological history; financial information (including assets, earnings and bank records) and evaluation records concerning a person's capability, recommendation, intellectual, formal, or informal education records.	
2	Are there any bills currently before parliament, or expected to come before parliament, that propose to amend the existing regime?	Currently, the House of Representatives is preparing a draft bill on Protection of Personal Data (**Bill**) as an overarching privacy law in Indonesia which is intended to replace the existing data protection provisions in Indonesian law. It is not clear when the Bill will be enacted. The Bill aims, among other things, to ensure 'that the transfer of personal data is conducted in a limited manner' (Article 3(d) of the Bill), especially the international transfer of data. **Further details of the Bill**	

#	Question	Response/Yes/No	Comment
		• The Preamble states that the protection of personal data is a human right that is protected by the Indonesian Constitution. • The Bill proposes to introduce a new Personal Data Protection Commission to implement the law and settle personal disputes out of court. • Article 1(4) proposes to make a distinction between 'Personal Data Controllers' and "Personal Data Processors'. • Article 8 requires consent from an individual to collect and process specific personal data. Draft Article 9 requires that consent to be in writing. • Article 35 prohibits the transfer of data outside of Indonesia unless the country of transfer has an Act with the same or more data protections, a contract is present between the parties or there is an international agreement with the transferring country. • Article 36 requires a person transferring data to an international third party to first obtain written consent from the data subject. • Article 53 will give the MCI authority to impose a wider range of administrative sanctions.	
3	What type of approach is this? • Consumer protection led? • Other?	The current and proposed Data Protection Laws take a consumer protection led approach, classifying the protection of personal data as both a constitutional and human right.[71] While this is the central aim, these Data Protection Laws also aim to protect the nations interest as evident in their broad application to data transfers that 'harm the interest' of Indonesia (Article 2 of MCI 11/2008).	

[71] Above n 1 145-146 [].

#	Question	Response/Yes/No	Comment
4	What is the scope of the law? • Telecoms? • Social media? • Media? • Medical? • Banking? • Other?	The current Indonesian Data Protection Laws are very broad, making any organisation that uses an electronic system to manage personal data subject to these laws.[72] Draft Article 1(4) of the Bill proposes to make a distinction between 'Personal Data Controllers', being a party that collects Personal Data (and obtains consent from the Data Owner) and manages the data processing, and 'Personal Data Processors', a party that processes the Personal Data on behalf of a Personal Data Controller. The Bill places more focus on Personal Data Controllers as the parties who should obtain the consent from the Personal Data Owner. Almost half of the relevant provisions under the Draft Law are on Personal Data management by Personal Data Controllers. As long as the scope of consent also allows Personal Data Processors to process the data, then Personal Data Processors do not need to obtain another consent from the Personal Data Owner. In any case, there is no requirement for a Personal Data Processor to obtain consent directly from the Personal Data Owner, and consequently the Personal Data Processors will rely on the Personal Data Controllers to obtain the appropriate consent (as is the case under the current regulations).	Any organisation, whether public or private, will be subject to these laws whether the data is used for internal or external purposes.
5	What does it imply in terms of data collection? • Do all types of data need to be captured, or only personal data?	The general Data Protection Laws only encapsulate Personal Data.[73] GR 82/2012 and MCI Regulation 20/2016 defines personal data as 'certain individual data relating to an individual, whose accuracy, confidentiality and protection must be ensured'. Further to this, the data must be attached and	There is no distinction between "specific data" and "non-specific data".

[72] Above n 1 149 [24].

[73] Above n 1 149 – 150 [26-29].

#	Question	Response/Yes/No	Comment
	How are they categorised? • Is the data stored by the commercial entity or by a public entity? • Is the data copied / sent to a public entity?	identifiable, either directly or indirectly, to an individual. [74] If this requirement is not present that data may fall beyond the application of the law.[75] Any personal data that is collected falls under the Indonesian law, regardless of the data owner's nationality.[76] **Financial Sector** ESPs in the Financial sector are required to store transaction data. Transaction data is an electronic transaction which has a legal consequence from using a computer, network or electronic media (GR 82/2012). Article 50 of POJK 69/2016 requires insurance and reinsurance companies to collect: • personal data of the policyholder, the insured or the participant; • data from premium payment transactions or claims; • population data and information; and • data and information in the administrative field of the legal entity.	
6	What does it imply in terms of data storage? • Does data have to be stored locally?	There are multiple regulations surrounding the localisation of data, with the main regulations surrounding ESPs that offer a 'public service' or offer a service in the financial sector. **Data Localisation for 'Public Service'**	The meaning of 'public service' has been interpreted widely to include services such as banking, insurance, health, transport, telecommunications and education:[81]

[74] Above n 1 150 [29].
[75] Above n 1 150 [29].
[76] Above n 1 150 [28].
[81] Above n 1, 154 [44].

#	Question	Response/Yes/No	Comment
	• Can data be stored outside of the country? • Can data stored locally be exported outside of the country? • Does that require an authorisation? • If so, by whom?	The definition of 'public service' is quite broad covering all institutions (state or independent) and corporations whose business relates to goods or services. GR 82/2012 and MCI 20/2016 require any organisation that provides a public service to locate the data and recovery centres in Indonesia. This data may be transferred internationally, however a copy must be kept in Indonesia.[77] Both GR 82/2012 and MCI 20/2016 must be consistent with Law GR 11/2008. Law GR 11/2008 applies to both those who reside in Indonesian and those who are outside the jurisdiction (to the extent that there is a legal implication in Indonesia or something harms an Indonesian national interest). Due to this, there has already been a request for a major foreign company to locate its data centre in Indonesia.[78] The MCI is proposing to ease the data localisation requirements and was preparing and amendment as at January 2016.[79] Further, the data localisation requirement may apply to foreign entities where the processing or storing of personal data will harm the national interest of Indonesia or has a legal implication within Indonesia.[80] **Data Localisation in the Financial Sector** All ESPs in the financial sector must store transaction data, being data that results from an electronic transaction in Indonesia. POJK 38/2016 and Article 50 of POJK 69/2016 require all banks, insurers and reinsurers to locate their data centres in Indonesia. There are some	• GR 96/2012 defines Public Service as an activity or chain of activities in terms of fulfilling the service needs in accordance with the law and regulation for every citizen and individual on goods, services, and / or administrative services that are provided by the public service operator. • Article 5 (1) of Law 25/2009 provides that the scope of public services includes public goods and services as well as administrative services. • Article 5(2) of Law 25/2009 further provides that this includes education, teaching, work and business, housing, communication and information, environment, health, social security, energy, banking, transportation, natural

[77] Above n 1 153 [41].
[78] Above n 1 155 [47].
[79] Above n 1 154 [44].
[80] Above n 1 156 [48].

#	Question	Response/Yes/No	Comment
		exceptions to these localisation rules for banks, provided that there is no data that contains identifiable customer information.	resources, tourism and other strategic sectors. This wide definition has been criticised and as a result the MCI is preparing an amendment that will ease localisation requirements.[82] An 'electronic transaction' is any action with legal consequence made by using a computer, computer network and/or electronic media (GR 82/2012).
7	What does it imply in terms of data processing? • Do the same processes apply to all data, or only to personal data? • Are these processes same for technical and commercial usage? • Can data be processed abroad? If so, does the data processor have to	Under the Data Protection Laws, unless exempted under other applicable laws or regulations, the prior express consent of the data subject must be obtained in order to process their personal data in an electronic system. The entity collecting such personal data is required to explain the purpose of the data use, processing, transfer and disclosure in detail in the consent document, and can only use or process such personal data based on the scope consented by the data subject. Consent must be given in written from, either in hard copy or through electronic means. (However, as a matter of practice, there is a likely possibility that the courts might not accept electronic consent as evidence and therefore it is recommended for entities to obtain a data subject's express consent in writing for evidentiary purposes.) **International Transfer of Data**	To transfer internationally, Article 22 of MCI/2016 requires: • an implementation plan of personal data transfer to be submitted to the MCI; • advocacy, meaning a request of advice from the MCI (if applicable); and • once the transfer has been completed, an implementation report to be submitted to the MCI within a certain time.

[82] Ibid.

#	Question	Response/Yes/No	Comment
	give mirror access locally? • How long is the data stored? • Is the data destructed after that period of time, or kept? • Is that monitored independently, or only by the State?	Articles 21 and 22 of MCI Regulation 20/2016 govern cross border data transfers, providing that an international transfer cannot take place unless the transferrer obtains the individual's consent and co-ordinates the transfer with the MCI. An ESP must notify the MCI of its plan to transfer the personal data outside Indonesia before the transfer. After the transfer, the ESP must submit a post-transfer report to the MCI, which must include details of the transfer. The notification to the MCI does not need to be made for each instance of cross-border transfer, and may include plans for several cross-border transfers in the future. Once passed, the Bill will apply this same default rule. However, draft Article 35 will impose further conditions which must be met to transfer data internationally.[83] Currently, the Data Protection Laws do not provide a requirement for the transferring country to have an adequate level of protection of personal data. However, Article 35 of the Bill prohibits the transfer of data outside of Indonesia unless: • the recipient jurisdiction affords an equal or greater level of protection as the Bill; • a contract exists between the parties; or • Indonesia has concluded an international agreement with the transferring country.	Advocacy will apply where the data subject exercises their right to advocacy. From here, the MCI will facilitate/mediate a settlement between the data subject and the facilitating party in an attempt to reach a favourable outcome for both parties. Article 22(1)(b) of the regulation requires the transfer to comply with cross-border personal data exchange legislation which, once the Bill is passed, will have full effect.
8	What does it imply in terms of data usage? • Can data be sold?	The entity collecting personal data is required to inform data subjects of how their personal data will be used and processed when collecting the data or before using or processing such personal data and before conducting any	

[83] Above n 1 148 [22].

#	Question	Response/Yes/No	Comment
	• Can statistical data be sold? • Can technical data be sold?	action in respect of personal data. Such personal data can only be used or processed based on the purposes consented to by the data subject. The Bill proposes sanctions for certain actions, such as personal data forgery and unauthorised sale of personal data.	
9	What control do people have on their data? • Are people informed of the data being collected? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) as a bulk? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) line by line? • How is that approval stored?	There are various articles surrounding both the collection and transfer of personal data. These have been detailed below. **Collection of Data** • There is no provision that requires an individual to expressly consent to opting-in to data collection.[84] • Article 15(1)(c) of GR 82/2012 requires any ESPs to ensure that any data collected, used or disclosed to be based on the consent from the data subject. • Once passed, Article 8 and 9 of the draft Data Protection Bill will require written consent from an individual before the collection and processing of specific personal data. **Transfer of data** • Article 6 and Article 1(4) of the MCI 20/2016 require an individual's consent for any transfer of personal data to a third party. This consent can only be given once the accuracy and confidentiality of the data has been confirmed by the individual. • Article 31 of Financial Service Authority Regulation Number 01/POJK 07/2013 provides that a consumer's personal data that has been collected in relation to any financial service cannot transfer data unless	The current consent requirement is not particularly onerous in practice, as companies only need to cover all transfers in the initial collection consent form.[85]

[84] Above n 1 151 [30].

[85] Above n 1 159 [64].

#	Question	Response/Yes/No	Comment
	• Who monitors it?	the consumer consents to it in writing or it is specifically required by a law. • Article 22(1) of MCI 20/2016 requires any cross-border data transfer to gain the subject matters consent after the accuracy of the data is verified, unless otherwise regulated by other laws. • Draft Article 36 of the Data Protection Bill will require a person transferring data internationally to obtain written consent from the data subject.	
10	Who is responsible for the implementation of the law? • NRA? • Ministry of ICT? • Army (or affiliate)? • Other?	The MCI is the implementing authority of existing Data Protection Laws. However, under the Bill a new Personal Data Protection Commission will be established and will be responsible for the implementation of the law and settling personal disputes out of court. The MCI handles all administrative sanctions for a breach of personal Data Protection Laws. Criminal sanctions are usually enforced by the police or a civil servant investigator from MCI.[86] Further, the OJK can impose sanctions surrounding financial sector specific data regulations.[87]	Note that the proposed Personal Data Protection Commission is still subject to change, and it is possible that the MCI could remain the enforcing body.
11	Who is responsible for possible breaches to the law? • Users?	Generally, it is 'electronic system operators', defined as any person, state official, business entity or society that provides, manages and/or operates, jointly or singly, an electronic system for the users of the electronic system for the operator's interest and/or others, that are subject to and liable under the Data Protection Laws.	

[86] Above n 1 161 [70].

[87] Above n 1, 148 [19-20].

#	Question	Response/Yes/No	Comment
	• Service provider? • Local operator? Just for themselves, or also on behalf of their counterparts? • Foreign operator / data handler?	The Data Protection Laws are silent on a local data exporter's liability where the overseas importer causes the breach. However, in principle, liability will always attach to an ESP who holds the data," allowing an importer to be liable.[88]	
12	Implications of breach • Risks to companies – Penalties – Loss of license – Other • Risks to people – Penalties – Arrest – Other	There are both administrative sanctions and criminal sanctions for a breach of the Data Protection Laws.[89] The administrative sanctions for the unlawful transfer or dissemination of person data can be either: • verbal warnings; • written warnings; • temporary suspension of business; and/or • publication online. Draft article 53 of the Bill will also allow administrative sanctions such as: • suspending processing; • removing or deleting the data;	The MCI will conduct an assessment for when to impose administrative sanctions. Where there are criminal sanctions involved, the standard criminal procedure will apply.

[88] Above n 1 159 [61].
[89] Above n 1 161 [70].

#	Question	Response/Yes/No	Comment
		• compensation payments; and/or • imposition of fines. The Criminal implications for the unlawful transfer of electronic information (this includes the electronic transfer of data without the data subject's consent) are: • a maximum eight years imprisonment; and/or • a Rp 2,000,000,000 fine. Further, a data subject may be able to gain compensation for a civil case under articles such as Article 26 of the EIT Law.	
13	Who monitors the correct implementation of the law • Parliament? • Consumer associations / civil society? • Nobody? • Other?	See the response to question 6 above.	

Country: Japan

Questionnaire

#	Question	Response/Yes/No	Comment
1	What is the relevant legislation? Are general data protection laws the only relevant laws or are there other sector specific laws as well that may impose additional requirements?	**Legislation** The Act on the Protection of Personal Information (**APPI**) is the main piece of legislation that provides personal data protections in Japan for private sector organisations. The public sector is regulated by a variety of local laws and ordinances. The Act on the Protection of Personal Information Held by Administrative Organs, the Act for the Protection of Personal Information Retained by Independent Administrative Institutions and the Unfair Competition Prevention Act, provide further protections surrounding personal information. **Policy** Attached to the APPI is the 'Basic Policy' on the Protection of Personal Information (**Basic Policy**) which was adopted by the Personal Information Protection Commission (**PPC**) in accordance with Article 7 of the APPI. **Guidelines** The PPC has also developed Guidelines on the APPI including: • Guidelines for the Act on the Protection of Personal Information (Provision to a Third Party in a Foreign Country Edition); • Guidelines for the Act on the Protection of Personal Information (General Rules Edition);	The Unfair Competition Prevention Act provides that trade secrets, which includes consumer lists, cannot be disclosed.

#	Question	Response/Yes/No	Comment
		• Guidelines for the Act on the Protection of Personal Information (Confirmation and Record-keeping Obligation at the Time of Third Party Provision); and • Guidelines for the Act on the Protection of Personal Information (Anonymously Processed Information Edition). The Guidelines for the Act on the Protection of Personal Information (Provision to a Third Party in a Foreign Country Edition) specify the restriction on the transfer of personal data to a foreign third party. **Standards** Standard JISQ1500, introduced by the Japanese Industrial Standard Committee also protects personal information when it relates to management systems. **Constitutional** Article 13 of the Japanese Constitution is widely interpreted to grant a right to privacy. **International** Japan is a member of multiple international agreements and frameworks, including: • the International Covenant on Civil and Political Rights (ratified); • the Asia-Pacific Economic Cooperation (**APEC**), APEC's Cross-border Privacy Enforcement Arrangement and APEC's Cross-Border Privacy Rules (**CBPR**); • the Global Privacy Enforcement Network;	Japan also has a system, PrivacyMark, which uses this standard as criteria that must be met in order to be certified for adequately handling personal information. A private organisation named JIPDEC operates this certification system.

#	Question	Response/Yes/No	Comment
		• the International Conference of Data Protection and Privacy Commissioners; • gaining observer status with the Council of Europe and the Consultative Committee of Convention; and • the G7 Principles and Action on Cyber. **Specific Sector Requirements** Finance, healthcare and IT have specific requirements for protecting personal data. Each of these sectors relevant Ministries have published Guidelines surrounding the protection of personal data.	JIPDEC is also the Accountability Agent for the APEC CBPR Scheme. Japan and the EU have mutually recognised the adequacy of each other's data protection laws however the European Commission's decision does not apply to transfers of data to academic institutions, religious bodies, media companies or political organisation except to the extent they are processed for academic, religious, journalistic or political purposes, respectively. The GDPR may also have effects on data processing activities in Japan, due to its extraterritorial reach.
2	Are there any bills currently before parliament, or expected to come before parliament,	No.	However, in January 2019, the EU and Japan mutually recognised each other's data protection laws as providing an

#	Question	Response/Yes/No	Comment
	that propose to amend the existing regime?		adequate level of protection of personal data.
3	What type of approach is this? • Consumer protection led? • Other?	The Basic Policy attempts to balance the '*smooth flow of data while ensuring the protection of personal information by participating in an international co-operative framework and building co-operative relations with foreign enforcement authorities'*.[90] The APPI is also centered around key themes of consumer protection and the promotion of a leading global economy.[91]	
4	What is the scope of the law? • Telecoms? • Social media? • Media? • Medical? • Banking? • Other?	The APPI applies to all 'personal information handling business operations'. Article 2 of the APPI defines a 'personal information handling business operation' as any person providing a personal information database for use in business, however, excludes central government organisations, local government organisations, incorporated administrative agencies and local incorporated administrative agencies. Further, Article 76 of the APPI lists press organisation, religious bodies, and political bodies as exceptions only for the purposes outlined in Article 76, which is to mean that they are exempt from the APPI to the extent the activity caught by the APPI is for the purposes of journalism, worship and political action. The APPI does not distinguish between 'controllers', 'processors' or 'intermediaries'.	
5	What does it imply in terms of data collection? • Do all types of data need to be	Personal data under the APPI, means personal information constituting a personal information database (Article 2 of the APPI).	

[90] Above n 1 165 [2].

[91] Above n 1 166 [5-6].

#	Question	Response/Yes/No	Comment
	captured, or only personal data? How are they categorised? • Is the data stored by the commercial entity or by a public entity? • Is the data copied / sent to a public entity?	Article 2 of the APPI defines 'personal information' as information relating to a living individual's: • name, date of birth, or other descriptions where an individual can be identified; and • identification code. Article 2 of the APPI defines a 'personal information database' to mean a collective body of information with an individual's personal information that can be searched for by a computer or has been prescribed by Cabinet to be systematically organised 'so as to be able to easily search for particular personal information.' Article 2 of the APPI also provides a definition for 'special care-required personal information', which relates to sensitive categories of information such as race, creed, social status, medical history etc. Article 3 of the Cabinet Order excludes information which will most likely not harm and individual's rights and interests. Personal Information includes information which can be collected with other information to identify an individual, even if the information concerned cannot be identified by itself.[92] **Anonymised Data** The APPI provides that even if the data is pseudonymised or encrypted, if it can identify an individual, it falls into the category of personal information.[93]	In 2017 the concept of 'anonymised information' was included in an amendment to the APPI which captures personal

[92] Above n 1, 173 [28].

[93] Above n 1 176 [35].

#	Question	Response/Yes/No	Comment
		Article 76 of the APPI applies to all personal information, regardless if the individual's origin is foreign or domestic. **Transfer of Data** Articles 23 and 24 of the APPI not only cover personal data but also 'special-care required information', meaning sensitive information as the provisions apply to 'personal data' not 'personal information'.	information that has been altered in a manner that means that it is irreversibly anonymised and the individual from whom it was collected is no longer identifiable. Where personal information meets the criteria specified in the amended APPI and is 'anonymised information', it is no longer personal identifiable information and subject to many of the requirements under the APPI, most notably consent requirements for data transfer.
6	What does it imply in terms of data storage? • Does data have to be stored locally? • Can data be stored outside of the country? • Can data stored locally be exported outside of the country?	**Data Localisation** Japan does not have data localisation requirements.[94] **Transfer of Data** Article 23 requires an individual's consent to be obtained before data can be transferred to a third party, there are however exceptions to this, including • where providing data is required by laws or regulations; • where it is necessary to communicate with government and gaining consent will interfere with this;	The Foreign Exchange and Foreign Trade Act impose a quasi-data localisation regulation as they restrict the international transfer of some types of data.[96]

[94] Above n 1 178 [42].

[96] Above n 1 178 [42].

#	Question	Response/Yes/No	Comment
	• Does that require an authorisation? • If so, by whom?	• where there is difficulty in gaining the individuals consent and it is necessary to: – protect an individual's life, body or property; and – enhance public hygiene or promote the sound development of children. Article 23(5) provides that there are certain circumstances which do not qualify a receiving party as a 'third party,' including where: • a personal information handling business operator is outsourcing some element of their processing operations within the scope of the original purpose of the processing; • where data is provided with business succession due to a merger or other reason; or • where the data subject has been informed of the data being used with other entities. As a rule, Article 24 of the APPI prohibits the international transfer of personal data, except where: • a third party transferee's country has a system recognised by the PPC Rules as having equivalent standards to Japan; • a third party has established a system that complies with the PPC Rules; or • the data subject's consent has been obtained.	

#	Question	Response/Yes/No	Comment
		Where an international transfer occurs, personal data can be provided in the same way it would be provided to a domestic third party (Article 24 of the APPI). The PPC Rules prescribe the standard which must be conformed to as: • complying with the APPI's obligations in an appropriate and rational manner; or • the importer holds a CBPR certification. Only the PPC is able to assess and prescribe a country as having comparable standards to Japan which is based off a set of 'judgemental standards'. These standards assess: • existing statute; • the relevant personal data protection authority and its policies, procedures and systems; • the necessity to recognise a foreign country as in Japan's national interest; • if co-operation is possible; and • whether a framework that both facilitates data transfer and protects personal data can be established.[95] The PPC's Guidelines for the Act on the Protection of Personal Information (Provision to a Third Party in a Foreign Country Edition) provides further guidance on the interpretation of Article 24.	The APPI applies generally to all international transfers, with no specific provision for data in transit.[97]

[95] Above n 1 182 [56].

[97] Above n 1 176 [34].

#	Question	Response/Yes/No	Comment
7	What does it imply in terms of data processing? • Do the same processes apply to all data, or only to personal data? • Are these processes same for technical and commercial usage? • Can data be processed abroad? If so, does the data processor have to give mirror access locally? • How long is the data stored? • Is the data destructed after that period of time, or kept? • Is that monitored independently, or only by the State?	Generally, under the APPI prior consent is needed before personal information can be processed overseas. Two exceptions apply: first, provided that the country where the data is to be processed requires at least the same level of data protection as required under the APPI, no consent is required. Secondly, if a written agreement with a third party located overseas requires that that party continuously undertake to handle the data with at least the same level of protection as required under the APPI, consent will also not be required. Article 2 of the APPI provides that users of data must promptly dispose of an personal identifiable information that is no longer required. Article 5 of the Amendment to the Cabinet Order to Enforce the APPI specifies that other types of information must be erased within 6 months.	

#	Question	Response/Yes/No	Comment
8	What does it imply in terms of data usage? • Can data be sold? • Can statistical data be sold? • Can technical data be sold?	The use of data is generally restricted to the purpose for which consent was obtained, however data may be disclosed provided that an opt-out mechanism is available and where the disclosure is for shared-use.	
9	What control do people have on their data? • Are people informed of the data being collected? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) as a bulk? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) line by line?	Any information that it anonymously processed information, can be both provided to a third party without consent and used for something other than its original purpose.[98] If either the processing method or security control measures allow for an individual to be identified, or personal information can be restored, this will not be the case. **Transfer of Data** Article 23 of the APPI requires an individual's consent to be gained before it can be transferred to a third party. There are however some exceptions to this provided for in Article 23(1), including: • where providing data is required by laws or regulations; • where it is necessary to communicate with government and gaining consent will interfere with this; • where there is difficulty in gaining the individuals consent and it is necessary to: – protect an individual's life, body or property; and	

[98] Above n 1 176 [36].

#	Question	Response/Yes/No	Comment
	• How is that approval stored? • Who monitors it?	– enhance public hygiene or promote the sound development of children. Article 24 prohibits the transfer of personal data to a foreign third party without an individual's consent. There are two exceptions to this rule, however, including where the transferee country has equivalent protection standards to Japan or the third party being transferred to has established a system that complies to the PPC Rules and APPI. Consent cannot be used to waive privacy safeguards in the transferee's country.[99]	
10	Who is responsible for the implementation of the law? • NRA? • Ministry of ICT? • Army (or affiliate)? • Other?	The PPC is the privacy enforcement authority and is responsible for the protection of personal data (per the Basic Policy).	The PPC is also responsible for implementing criteria to assess and assessing the standards of other jurisdictions for the equivalency exemption in Article 24 (transfer of data internationally).[100]
11	Who is responsible for possible breaches to the law?	The APPI provides that a local data exporter will remain liable where a foreign data importer breaches the personal data laws. This will only occur where the transfer occurred for the purpose of outsourcing personal data processing or	Note that any breach of the Guidelines and their corresponding obligations will be a breach of law.[102]

[99] Above n 1 183 [59].
[100] Above n 1 183 [57].
[102] Above n 1 172 [26].

#	Question	Response/Yes/No	Comment
	• Users? • Service provider? • Local operator? Just for themselves, or also on behalf of their counterparts? • Foreign operator / data handler?	the local exporter has ensured that the importers country has a standard of rules equal to the PPC Rules and APPI.[101] Thus, even if responsibility is imposed on the foreign data importer, the local data exporter will not be exempt.	
12	Implications of breach • Risks to companies – Penalties – Loss of license – Other • Risks to people – Penalties – Arrest – Other	The APPI does not specifically attach any sanctions where a breach occurs, however the PPC holds enforcement powers for any breach of Article 24. The Unfair Competition Prevention Act, imposes criminal sanctions on individuals who disclose trade secrets, which includes disclosing consumer lists and relevant personal information.	

[101] Above n 1 180 [49].

#	Question	Response/Yes/No	Comment
13	Who monitors the correct implementation of the law • Parliament? • Consumer associations / civil society? • Nobody? • Other?	The PPC is the independent privacy enforcement authority and is responsible for the protection of personal data (per the Basic Policy). The Commission produces guidance materials and advice with respect to the correct implementation of the APPI.	

Country: Singapore

Questionnaire

#	Question	Response: Yes/No	Comment
1	What is the relevant legislation? Are general data protection laws the only relevant laws or are there other sector specific laws as well that may impose additional requirements?	Singapore's data protection laws are made up of common law rights, sector specific legislation as well as legislation governing the protection of personal information. **Legalisation (Data Protection)** The Personal Data Protection Act (**PDPA**) is the overarching legislation for data protection. • The PDPA applies to the private sector, with section 4(1)(c) specifically providing that the PDPA does not apply to Government. • Section 10(3) provides that the Personal Data Protection Commission (**PDPC**) cannot give information to a foreign protection body unless the foreign body gives a written undertaking that it will comply with section 10 of the PDPA and relevant laws concerning this. • Section 59 provides that where a foreign co-operation agreement has been reached under section 10 of the PDPA, the PDPC can then can disclose information which is necessary to comply with the agreement. Section 59(6) provides that to satisfy this requirement the information requested must be: – in possession of the Commission; – provided with an undertaking to keep the information given confidential (unless the Government allows otherwise); and	The 'information necessary' to comply with the agreement may include information from investigations or assistance in cross-border investigations.

#	Question	Response: Yes/No	Comment
		– not contrary to public interest. • Section 26 prohibits the international transfer of data, however there are some exceptions to this rule (see below). **Legislation (Other)** • Computer Misuse Act • Cybersecurity Act • Spam Control Act • Electronic Transactions Act **Regulations** Multiple regulations have been passed under the PDPA, including: • The Personal Data Protection (Appeal) Regulations 2015; • The Personal Data Protection Regulations 2014 (**PDPA Regulations**); • The Personal Data Protection (Enforcement) Regulations 2014 (**Enforcement Regulations**); • The Personal Data Protection (Do Not Call Registry) Regulations 2013; and • The Personal Data Protection (Composition of Offences) Regulations 2013. *PDPA Regulations*	

#	Question	Response: Yes/No	Comment
		• Part III sets out some of the exemptions to the section 26 rule and provides multiple requirements which must be met in order to transfer personal data internationally. **Guidelines** The PDPC has developed Advisory Guidelines on the Key Concepts in the Personal Data Protection Act. These guidelines include: • Guidance on the transfer limitation obligation in Chapter 19 of the PDPA; and • Sector specific guidelines such as guidance on the Healthcare, education and telecommunications sectors. **International Conventions** In order to support its position as an international data hub, Singapore participates in multiple international schemes, these include: • the Asia-Pacific Economic Cooperation(**APEC)** Cross Border Protection Rules (**CBPR**) which Singapore joined in 2018; • APEC's Privacy Recognition for Processors (**PRP**) (also from 2018) • APEC's Cross-Border Privacy Enforcement Arrangement (**CPEA**); • the Joint Oversight Panel (**JOP**); and • a member state to the Association of Southeast Asian Nations (**ASEAN**) Human Rights Declaration and Economic Community.	

#	Question	Response: Yes/No	Comment
		Singapore also has 21 free trade agreements with 32 trading partners, which deal with data protection issues.[103] These free trade agreements vary in the protections they provide surrounding data and the extent to which they provide protection for data. **Constitutional Protections** Article 9(1) of Singapore's Constitution provides that 'no personal shall be deprived of his life or personal liberty, save in accordance with law'. This is identical to India's constitution, which a recent case[104] interpreted to include privacy. This has not been tested in Singapore. **Sector Specific laws** The Financial sector has legislation that works in conjunction with the PDPA to form the data protection laws in this sector. This legislation includes: • the Banking Act Cap 19, 2008 Rev Ed (**Banking Act**); and • the Insurance Act Cap 142, 2002 Rev Ed (**Insurance Act**). Further, Singapore has a Free Trade Agreement with Europe (EUSFTA) which contains specific provisions on the transferring and protection of personal data for financial services (Article 8.54). **Banking Act** Attached to the Banking Act is the Banking Secrecy Outsourcing Conditions issued by the Monetary Authority of Singapore (**MAS**) and the MAS Guidelines on Outsourcing.	

[103] Dr Clarisse Girot, Regulation of Cross-Border Transfers of Personal Data In Asia, Asian Business Law Institute, 324 [38]; these include the EU, Australia, Japan, Asia Pacific and China.
[104] *Justice K S Puttaswamy v Union of India* 1999 Rev Ed.

#	Question	Response: Yes/No	Comment
		• MAS Notice 634 of these conditions require that consumer information is kept confidential and protected from all outsourcing arrangements to service providers. • Paragraph 5.10 of the MAS Guidelines: – allows for the use of data centres outside of Singapore, however, restricts the types of service providers that can be outsourced to; – provides detailed considerations which must be given by the outsourcing institution; and – requires confirmation to be given in writing to MAS to inspect the service provider. Paragraph 5.10.2(c) of the MAS Guidelines requires notification to be given to MAS where the overseas provided seeks authority to restrict or deny the rights of the Singapore institution or MAS.	
2	Are there any bills currently before parliament, or expected to come before parliament, that propose to amend the existing regime?	None.	
3	What type of approach is this? • Consumer protection led? • Other?	While consumer protection laws are a focus of Singapore's data protection laws, the main position taken by the Singapore government is economic.[105] As a trusted international data hub, Singapore introduced high data protection standards to create a system that 'affords trust in [the] national institution and seamless integration into global networks'.[106] Due to this, the regulations	

[105] Dr Clarisse Girot, Regulation of Cross-Border Transfers of Personal Data In Asia, Asian Business Law Institute, 315 [1] and 318 [11].

[106] Above n 1 317 [8].

#	Question	Response: Yes/No	Comment
		introduced by Singapore focus heavily on the regulation of international data.[107]	
4	What is the scope of the law? • Telecoms? • Social media? • Media? • Medical? • Banking? • Other?	The PDPA only provides data protection in the private sector, section 4(1)(c) of the Act provides that it does not apply to Government. The PDPA does not exempt certain sectors or companies form the Act,[108] implying that it will apply to all private sector organisations. However it should be noted that some sector specific legislation also carries certain obligations with respect to data protection such as the Telecom Competition Code issued under the Telecommunications Act Cap 323. The PDPA also has extraterritorial reach so this may affect organisations located outside of Singapore.[109]	
5	What does it imply in terms of data collection? • Do all types of data need to be captured, or only personal data? How are they categorised? • Is the data stored by the commercial entity or by a public entity?	The PDPA covers personal data, which is defined as data, whether true or not, about an individual who can be identified from that data, or from the data and other information to which the organisation has or is likely to have access. Chapter 11 of the PDPC Advisory Guidelines suggests that this is any data of an individual collected both inside and outside of Singapore. Data that is anonymised may not be in the scope of the definition of 'personal data'. A 'Data intermediary', an entity that processes information on behalf of another information under a written agreement, may be exempt from many of the obligations under the PDPA.	If an organisation has information that could re-identify the individual, the dataset will not be treated as anonymised and will be protected by the PDPA.[110]

[107] Above n 1 318 [12].
[108] Above n 329 [57].
[109] Above n 1 327 [50].
[110] Above n 1 239 [56].

#	Question	Response: Yes/No	Comment
	• Is the data copied / sent to a public entity?	Section 4 of the PDPA provides that business contact information and data of deceased individuals is not included.	
6	What does it imply in terms of data storage? • Does data have to be stored locally? • Can data be stored outside of the country? • Can data stored locally be exported outside of the country? • Does that require an authorisation? • If so, by whom?	**Where Can Data be Stored?** Singapore has no data localisation requirements.[111] *Banking Sector* • Paragraph 5.10 of the MAS Guidelines allows for the use of data centres outside of Singapore, however, it provides that institutions need to consider 'applicable government policies, political, social and economic conditions, legal and regulatory developments and the institution's ability to effectively monitor the service provider'.[112] • Paragraph 5.10.2 of the MAS Guidelines places a higher standard on services providers who have an outsourcing agreement. These guidelines provide where this is an international outsourcing agreement that the outsourcing cannot hinder MAS' efforts to monitor the Singapore institution in a timely manner.[113] Further the bank needs to confirm in writing to MAS that it has the right to inspect the service provider and its information, reports and findings relating to the outsourcing agreement (paragraph 5.10.29(b)). **Transfer of Data** Section 26 of the PDPA forbids the international transfer or data. This law has extraterritorial effect, so this may affect organisations located outside of Singapore.	An outsourcing agreement as defined by paragraph 3.1 of the MAS Guidelines is an arrangement which may materially impact an institution or its customers. The PDPA defines an organisation as 'any individual, company, association or body of persons corporate or unincorporated, whether

[111] Above n 1 327 [48].
[112] Above n 1 321 [24].
[113] Above n 1 322 [26].

#	Question	Response: Yes/No	Comment
		There are some exceptions to this including where: • the organisation applies to the PDPC by written notice for exemption (section 26(2)); • the data subject consents (limited by PDPA Regulation 9);[114] • the data is publicly available (PDPA Regulation 9); • where the data is in transit through Singapore (PDPA Regulation 9); • the transfer of data is necessary for the performance of a contract, even where a third party is involved (there are some limitations to this exemption);[115] or • where the transferring organisation takes steps to ensure that the data will not be used or disclosed by the transferee, it can be disclosed where: – is in the interest of the individual and consent cannot be obtained in a timely manner; – is responding to an emergency that threatens the life or safety of an individual; – is in the national interest; or – is to contact the next of kin to an injured or deceased individual.[116]	or not – (a) formed or recognised under the law of Singapore; or (b) resident, or having an office or a place of business, in Singapore'. Regulation 9 provides consent cannot be used as an exemption where: - the individual was not given a reasonable summary of the extent to which their data will be protected; - the consent was required as a condition of using the product (unless the transfer is reasonably necessary to provide the

[114] Above n 1 330 [62].
[115] Above n 1 334 [76].
[116] Above n 1 334 [77].

#	Question	Response: Yes/No	Comment
		Further, where the data is anonymised, it may fall outside the scope of the PDPA, and therefore the data may be freely transferred overseas. Part III of the PDPA regulations set out the requirements which must be met in order to transfer personal data to another country. These requirements include the use of a contractual agreement that ensures that a comparable standard of protection is provided by the transferee.[117] Section 26(2) allows for the PDPC to provide an exemption to this requirement. Where data is transferred, PDPA Regulation 9 requires the transferring organisation to: • ensure that the data is collected in compliance with Parts III and VI of the PDPA; and • ensure that the recipient is legally bound by a standard of protection comparable to the PDPA. This standard of protection can be imposed by local laws of the country of transfer, a contract, binding corporate rules or any legally binding instrument (PDPA Regulation 9 and 10). There are no current white or black lists which list countries compared to the Singapore standards.[118] **Financial Sector** The financial sector has a specific regime which applies to cross-border transfers which is regulated by MAS.[119]	product or service); or - the information was obtained as a result of deceptive or misleading conduct. Section 2(1) of the PDPA defines 'publicly available data' as personal data that is generally available to the public. Contractual Agreements are the most commonly used exemption.[120] The PDPC published a Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data, which provides a template which parties can use to establish cross-border data transfers.

[117] Above n 1 320 [18].
[118] Above n 1 332 [65-70].
[119] Above n 1 321 [22].
[120] Above n 1 335 [79].

#	Question	Response: Yes/No	Comment
7	What does it imply in terms of data processing? • Do the same processes apply to all data, or only to personal data? • Are these processes same for technical and commercial usage? • Can data be processed abroad? If so, does the data processor have to give mirror access locally? • How long is the data stored? • Is the data destructed after that period of time, or kept? • Is that monitored independently, or only by the State?	The processing of personal data is captured by the expression 'collection, use and disclosure' under the PDPA. The informed consent of the individual is required prior to the 'collection, use or disclosure' of personal information (unless as otherwise permitted by law). The PDPA does not classify personal data however section 24 of the PDPA does require that an organisation consider 'reasonable security arrangements' with respect to preventing unauthorised access to personal data as well as its modification and disposal, which may vary relative to the sensitivity of the information collected. Anonymised data is not personal data (according to the PDPC's "advisory guidelines on the Personal Data Protection Act for Selected Topics"),[121] and may not be subject to the data protection provisions under Parts III to VI under the PDPA applying to the collection, use or disclosure of personal data. Section 25 of the PDPA provides that organisations should only retain personal data for as long as required for the purposes for which it was collected or for legal or business purposes. Singapore has no data localisation requirements.[122] There are strict requirements on the transfer of data overseas (see above). However, if the exemption criteria is met, there is nothing prohibiting overseas data processing. It is worth noting that Section 4(3) of the PDPA provides that a local data holder can be liable for a breach caused by an overseas service provider as the local entity is subject to the same obligation as if it were processed by itself.	

[121] Above n 1 329 [55]

[122] Above n 1 327 [48].

#	Question	Response: Yes/No	Comment
8	What does it imply in terms of data usage? • Can data be sold? • Can statistical data be sold? • Can technical data be sold?	The PDPA requires an individual's consent (section 13) for the 'collection, use and disclosure' of personal data. An organisation may use personal data consistent with the consent they have obtained from the individual from who it was collected or where an exception applies under the PDPA (including where the data is anonymised and no longer meets the definition of 'personal data' under the PDPA).	
9	What control do people have on their data? • Are people informed of the data being collected? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) as a bulk? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) line by line? • How is that approval stored? • Who monitors it?	Section 13 of the PDPA requires that consent be obtained for the 'collection, use and disclosure' of personal information (unless an exception applies) meaning that notification to an individual is required. Section 16 of the PDPA permits individuals to withdraw their consent (with reasonable notice) for their information being held by an organisation. Consent can be used as an exemption to the section 26 rule of the PDPA, so that data can be transferred internationally.[123] Where consent is used for this purpose, the privacy safeguards (PDPA Regulation 9(4)(a)) still apply. The Advisory Guidelines on Key Concepts in the PDPA notes that organisation should have controls and processes in place for the proper recording and storage of all personal data they hold, in an unstructured form.	

[123] Above n 1 332 [71].

#	Question	Response: Yes/No	Comment
10	Who is responsible for the implementation of the law? • NRA? • Ministry of ICT? • Army (or affiliate)? • Other?	The PDPC is the privacy enforcement authority for Singapore and is responsible for the implementation of the PDPA. This includes the implementation of the international data transfer rules. The PDPC will investigate, assess and impose sanctions on organisations who breach the transfer limitation obligations.[124] **Financial Sector** Within the Financial Sector the MAS will enforce banking secrecy obligations under the Banking Act.	
11	Who is responsible for possible breaches to the law? • Users? • Service provider? • Local operator? Just for themselves, or also on behalf of their counterparts? • Foreign operator / data handler?	The PDPA applies to any individual, company, association or body of persons, corporate or unincorporated, whether located in or outside Singapore (**Organisations**). It is Organisations who are liable for breaches to the PDPA. The PDPA also contains the concept of data intermediaries (a concept similar to that of data processors in the EU). Where a data intermediary processes personal data under a contract in writing with an organisation and for the purposes of that organisation, it will be largely exempt from the PDPA and only subject to the security and retention obligations contained in the PDPA. Section 4(3) of the PDPA provides that a local data holder can be liable for a breach caused by an overseas service provider as the local entity is subject to the same obligation as if it were processed by itself.	
12	Implications of breach • Risks to companies	**Local** Section 29(1) of the PDPA states that the PDPC can give an organisation breaching Parts III and VI of the PDPA a direction, including to:	

[124] Above n 1 320 [20].

#	Question	Response: Yes/No	Comment
	– Penalties – Loss of license – Other • Risks to people – Penalties – Arrest – Other	• stop collecting, using or disclosing the data in contravention of the PDPA; • destroy data collected in contravention of the PDPA; • comply with any direction of the Commission under section 28(2); or • pay a fine of up to $1 million dollars. Generally, the PDPC will only take enforcement action where an organisation cannot resolve the issue they have with the data subject, where multiple people have been affected, if the contravention was intentional or there were no policies to ensure compliance with the PDPA.[125] **Global** Singapore also participates in APEC's CPEA and Global Privacy Enforcement Network.	
13	Who monitors the correct implementation of the law • Parliament? • Consumer associations / civil society? • Nobody? • Other?	Parliament of Singapore Personal Data Protection Commission	

[125] Above n 1 339 [100].

Country: South Korea

Questionnaire

#	Question	Response/Yes/No	Comment
1	What is the relevant legislation? Are general data protection laws the only relevant laws or are there other sector specific laws as well that may impose additional requirements?	South Korea's data protection laws are some of the strictest in the world. The regime is comprised of multiple pieces of legislation (detailed below). **Legislation** The Personal Information Protection Act (**PIP Act**) introduced in 2011 and the Act on the Promotion of Information Communication Network Usage and Information Protection (**Network Act**) are the key legislative protections for personal data in South Korea. **Constitutional Protections** Korea's constitution references privacy several times, with Article 10 and 17 providing the key privacy protections. These articles have been interpreted to include the protection and privacy of data by multiple jurisdictions throughout Korea[126] with the Constitutional Court holding that citizens have a 'right to self-determination of personal data.'[127] From this right of self-determination multiple other rights have been derived, including: • the right to only have personal data collected or used with consent; • the right to access and correct personal information;	Article 10 of the Korean constitution states 'all citizens shall be assured of human worth and dignity and have the right to pursue happiness.' Article 17 of the Korean constitution states 'the privacy of the citizen shall not be breached.'

[126] Dr Clarisse Girot, Regulation of Cross-Border Transfers of Personal Data In Asia, Asian Business Law Institute, 348 [23].

[127] *Case 17-1* KCCR 668, 99Hun-Ma513 and 2004Hun-Ma190 (26 May 2005).

#	Question	Response/Yes/No	Comment
		• the right to stop the collection and usage of personal data; and • the right to request personal data to be destroyed.[128] **Criminal Code** Korea's Criminal Code makes it an offence to open or learn the contents of any letter, document or drawing that is sealed or designed to be secret, including electronic records. **Communications Privacy Protection Act (CPPA)** The CPPA makes it a criminal offence to record the contents of any transmission or reception of all kinds of sounds, words, symbols or images by any electromagnetic system, including telephone and email. **Sector Specific Protections** If applicable, any of the sector specific laws generally take precedence over the PIP Act and Network Act. **Financial Sector** The Act on the Use and Protection of Credit Information regulates both personal and corporate credit information. The Credit Information Act, Bank Act, Act on Insurance Business, the Electronic Financial Transaction Act and the Financial Services Commission Regulations also provide specific cybersecurity requirements which must be met. The finance sector also has data localisation restrictions (provided by the Credit Information Act), outsourcing restrictions (provided by the Regulation on Financial	

[128] Above n 1, 349 [24].

#	Question	Response/Yes/No	Comment
		Institutions' Outsourcing of Data Processing Business & IT Facilities) and is generally prohibited from transferring personal data overseas.[129] **Health Sector** The Medical Service Act and Protection and the Use of Location Information Act protect electronic health records. The Enforcement Rule of the Medical Service Act and the Standards of Facilities and Equipment for Management and Retention of Electronic Medical Records require data to be localised and prohibit the transfer of data to an overseas location. **Online Service Providers** The Network Act provides different security requirements for online service providers. **Communications Sector** The Act on Promotion of Information and Communications Network Utilisation and Information Protection governs information and communications service providers. **Personal Location Information** Personal location information is protected by the Act on the Protection and Use of Location Information. **Guidelines** While not binding, there are multiple guidelines which have been published by regulating authorities including:	

[129] Above n 1, 365 [83].

#	Question	Response/Yes/No	Comment
		• the Ministry of Interior and Safety's guidelines on the PIP Act; • Personal Information Protection Commission (**PIPC**) guidelines on the protection laws; • the Guidelines on Personal Information De-Identification Measures, which has been jointly adopted by multiple enforcement agencies. **International Protections** Two of South Korea's enforcement agencies, specifically the PIPC and Korea Internet and Security Agency (**KISA**) are members of the International Conference of Data Protection and Privacy Commissioners and participate in the Global Privacy Enforcement Network. Further, two other regulatory bodies, the PIPC and Ministry of Interior and Safety have joined the Cross-border Privacy Enforcement Arrangement. Korea is also: • a member of the International Covenant on Civil and Political Rights (**ICCPR**); • an observer of the Consultative Committee of the Council of Europe Convention 108; and • a member of Asia-Pacific Economic Cooperation (**APEC**) and the APEC Cross-border Privacy Rules. Further Korea has signed multiple bilateral and multilateral free trade agreements (**FTA**), including: • the Korea-ASEAN FTA; • the Korea-EU FTA; and	Korea has initiated the process to be recognised by the EU as a country that provides an adequate level of data protection under Directive 95/45/EC.

#	Question	Response/Yes/No	Comment
		• the Korea-US FTA. **Specific Rules** Specific rules surround sensitive personal information. This includes information that is likely to do harm to the privacy of data subjects (Article 23 of the PIP Act).	
2	Are there any bills currently before parliament, or expected to come before parliament, that propose to amend the existing regime?	There is currently a bill to amend the provisions in relation to the transfer of data in the Network Act. These amendments are being made in response to recent developments, communications with the EU Commission and to make steps to join APEC CBPRs. [130] The reforms proposed by this bill will bind an overseas recipient to the same standards as a local transferrer and will allow the PIPC to have authority to suspend the international transfer of data if 'the users' rights are severely violated'.[131] Further exemptions to the consent requirement would also be introduced by this bill including where Korea is a party to other international agreements or where the recipient has a certified Personal Information Management System .	
3	What type of approach is this? • Consumer protection led? • Other?	Korea has taken a strict consumer led approach to its data protection laws, enshrining the right to privacy and with that, the right to have control over personal data, as a fundamental right within its constitution.[132]	

[130] Above n 1, 357 [51].

[131] Above n 1, 357 [51].

[132]Above n 1, 343 [2].

#	Question	Response/Yes/No	Comment
4	What is the scope of the law? • Telecoms? • Social media? • Media? • Medical? • Banking? • Other?	**Scope of the Acts** The PIP Act regulates every area of personal information processing held by Korean companies. The PIP Act uses the term “personal information managers" to mean a public institution, corporate body, organisation or individual who manages personal information directly or via another person. It is also has the concept of a “data consignee”, who is a person who is delegated with the responsibility to process personal information, and is only responsible for compliance with more limited aspects of the PIP Act. The Network Act regulates personal information processed by information and communications service providers (**ICSPs**). ICSPs are defined in the act as telecommunication operators, providers of information or intermediate information providers who commercially use the services rendered by telecommunications operators. The difference between the Network Act and the PIP Act is generally that the Network Act regulates online activities and the PIP Act regulates mostly offline activities. Both the PIP Act and Network Act do not state the territorial scope of their application, however, the PIPC has stated that the Network Act will be applicable to receiving foreign service providers. The consent requirements when transferring internationally under the Network Act apply when: • transferring to a third party for their benefit (this includes where personal Korean information is accessed from abroad);	The PIP Act and Network Act define ‘personal information’ quite similarly. These definitions include information relating to a living individual that makes it possible to identify them by their name, registration number or image (this includes information that when combined with other information could identify the individual) (Article 2 of the PIP Act and Article 6 of the Network Act). Data that is anonymised will not be in the scope of these acts, however, if the data could be re-identified it will be subject to these acts. It is generally understood that the personal data of foreign citizens are afforded the same protections as a local individual’s personal data, if that data is controlled or processed in Korea.[133]

[133] Above n 1, 364 [79].

#	Question	Response/Yes/No	Comment
		• a service provider is outsourcing processing of data; or • when personal data is stored outside of Korea. It is unclear whether these acts will apply to data in transit. Both the PIP Act and Network Act do not exempt any specific sector or company, so these data protection laws are applicable to all public and private organisations.	
5	What does it imply in terms of data collection? • Do all types of data need to be captured, or only personal data? How are they categorised? • Is the data stored by the commercial entity or by a public entity? • Is the data copied / sent to a public entity?	The PIP Act provides that only the minimum amount of personal data necessary for an approved purpose should be collected. Resident Registration Numbers may only be collected if specifically required or permitted by a law or regulation, or if there exists a clear and urgent need to do so to protect the life, physical or economic interest of the subject of the data or a third party. Generally, registration or notification to the subject of personal information requirements only apply when the data is personally identifiable.	
6	What does it imply in terms of data storage? • Does data have to be stored locally?	**Data Localisation** Generally, Korean data protection rules do not provide for data localisation requirements. However, this varies from sector to sector.	

#	Question	Response/Yes/No	Comment
	• Can data be stored outside of the country? • Can data stored locally be exported outside of the country? • Does that require an authorisation? • If so, by whom?	The financial and health sectors are two sectors that have data localisation requirements. **Transfer of Data** Article 17 of the PIP Act requires the consent of a data subject to transfer data either domestically or internationally. There are exceptions to this held within article 17(1) and 15(1) of the PIP Act, specifically where the transfer corresponds with the initial reason for collection and is needed: • to comply with a legal obligation; • by a public institution to perform its notional statutory mission; or • to protect a human life or economic interest from impending danger, where that data subject cannot consent. When transferring data overseas, the transferring and receiving service provider must agree to protective measures and these must be included in a contract between the parties (Article 63(4) of the Network Act). These measures are defined by Presidential Decree, specifically including technical and administrative measures, measures to deal with disputes between parties and anything else necessary for protection of data. The financial sector prohibits the transferring of data overseas.	
7	What does it imply in terms of data processing? • Do the same processes apply to	**Overseas Processing** The PIP Act does not separately address the transfer of personal information abroad. However, the transfer of personal information abroad requires consent from the information subject under the provisions requiring consent prior to any transfer of personal information to a third party.	

#	Question	Response/Yes/No	Comment
	all data, or only to personal data? • Are these processes same for technical and commercial usage? • Can data be processed abroad? If so, does the data processor have to give mirror access locally? • How long is the data stored? • Is the data destructed after that period of time, or kept? • Is that monitored independently, or only by the State?	The Network Act requires that any transfer of personal information abroad must be preceded by not only consent but also certain technical, managerial and physical protection measures. *Financial Sector* Data can only be processed overseas if it has a limited effect on the security and reliability of electronic transactions. These overseas processers cannot process any identification information or personal credit information covered in the Credit Information Act. Due to this, financial providers are essentially required to process data in Korea. **Data Storage Length** Article 17(1) of the PIP Act requires the service provider to inform the data subject of how long an international recipient of transferred data will hold the data for.	
8	What does it imply in terms of data usage? • Can data be sold? • Can statistical data be sold?	The PIP Act contains eight Personal Information Protection Principles. They require personal information to be collected for specific and lawful purposes and not used for further incompatible purposes. A personal information manager may use personal information for a new purpose or provide personal information to a new third person if doing so does not infringe the	

#	Question	Response/Yes/No	Comment
	• Can technical data be sold?	interests of an information subject or a third person and one of the following conditions is satisfied. The conditions for further processing are: • the information subject consents; • special provisions exist in any other Act; • where it is obviously necessary for the physical safety and property interests of an information subject or a third person and it is not possible to obtain consent; or • where personal information is necessary for the compiling of statistics or for scientific research purposes and the personal information is provided in a form by which a specific individual cannot be identified. Additional conditions apply where the processing is by a public agency. The PIP Act also has specific rules applicable to business transfers and other corporate transactions.	
9	What control do people have on their data? • Are people informed of the data being collected? • Are people capable of accepting (= they want it) or rejecting (= they	There are explicit opt-in consent requirements for the processing of data within the public and private sectors in order to provide individuals with their constitutional right to privacy. There are some exceptions to this for both the private and public sector (more liberally given in the public sector).[134]	

[134] Above n 1, 346 [15].

#	Question	Response/Yes/No	Comment
	don't want it) as a bulk? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) line by line? • How is that approval stored? • Who monitors it?	**Transfer of Data** Article 17(1) of the PIP Act requires the data provider to gain consent from a data subject before any transfer of personal data takes place.[135] When obtaining this consent, the data provider must notify the data subject of: • who the data will be transferred to; • what purposes the recipient will use this information for; • details of what will be provided; • the period the recipient will have the data for; and • their right to not give their consent and any negative consequence from not allowing this transfer of data. If there are any changes to the above criteria, the data subject must also be informed (Article 17(2) of the PIP Act). Article 22 of the PIP Act also prescribes the method for obtaining this consent, specifically that requests for consent must be: • in a recognisable manner which distinguishes consent from other matters; and • obtained separately for original collection, the provision to a third party, the processing of sensitive information and for processing national identifiers. **International Transfer of Data** A separate consent is required to transfer personal data overseas (Article 17(3) of the PIP Act). Both the Korean service provider and international receiver must	

[135] Above n 1, 346 [17].

#	Question	Response/Yes/No	Comment
		obtain the data subjects consent (Article 63(2) of the Network Act). This consent can only be obtained where the data subject is informed of: • what is being transferred; • the country it is to be transferred to; • how and when it will be transferred; • the name of who the information is being transferred to; • what purposes the recipient will use this information for; and • the period which the data will be retained and used (Article 63(3) of the Network Act). There are exceptions to this held within section 63(2) of the Network Act, including where: • an agreement between the transferring and receiving party has been entered into; • the international transfer is necessary to better user convenience; and • the service provider has disclosed, either via its policy or individual notification prescribed by statute, the requirements under Article 63(3) (see above).	The PIP Act only requires consent when transferred from a local data controller to an overseas controller not from a local data controller to overseas processor.[137] The Network Act requires consent for any transfer.

[137] Above n 1, 361 [66].

#	Question	Response/Yes/No	Comment
		Privacy Safeguards Overseas Consent cannot be used to waive the requirement to put privacy protections in place in the receiving party's country.[136]	
10	Who is responsible for the implementation of the law? • NRA? • Ministry of ICT? • Army (or affiliate)? • Other?	South Korea has multiple agencies/authorities who are responsible for the enforcement of data privacy protections. The Ministry of the Interior and Safety (**MOIS**) is responsible for the enforcement of the PIP Act. The Personal Information Protection Commission (**PIPC**) is responsible for enforcing the Network Act. The Korea Internet and Security Agency (**KISA**) is the main agency responsible for enforcing breaches to privacy protections and internet security (this includes the transfer of data internationally). This is due to the MOIS and PIPC entrusting KISA with the actual handling of investigations. These three organisations above are able to conduct investigations, demand the production of documents and conduct on-site inspections.[138] Where there are sector specific laws, there are different regulatory authorities responsible for enforcing those laws.[139] In particular, the Financial Services Commission is responsible for enforcing the Credit Information Act, and issues formal interpretations of that Act. Further, the data protection laws enable the privacy regulators in Korea to assist and cooperate with privacy regulators in other jurisdictions (Article 14 of the PIP Act and Article 62 of the Network Act).	Although it has not yet been decided, it is likely that the Korea Internet and Security Agency will play the role of the CBPR Administrative Authority. KISA is also the certification agency for the PIMS scheme and the Information Security Management System Scheme.

[136] Above n 1, 373 [121].
[138] Above n 1, 381 [162].
[139] Above n 1, 345 [8].

#	Question	Response/Yes/No	Comment
11	Who is responsible for possible breaches to the law? • Users? • Service provider? • Local operator? Just for themselves, or also on behalf of their counterparts? • Foreign operator / data handler?	Generally, “personal information managers" – meaning public institutions, corporate bodies, organisations or individuals who manage personal information. Korean data exporters are liable where there has been a breach by the data importer overseas.[140]	
12	Implications of breach • Risks to companies – Penalties – Loss of license – Other • Risks to people – Penalties	There are no prescribed sanctions or penalties for the breach of provisions relating to cross-border transfers in the PIP Act. The Network Act introduced some penalties in its 2016 amendment. • The penalties introduced in the amendment to the Network Act include: • a penalty of up to 3% of sales revenue related to the violative activity may be imposed where an ICSP transfers information without consent; • a fine of up to KRW20m for the transfer of personal information to an overseas processer without proper notice or disclosure; • a corrective order issued against a ICSP for a breach of the Network Act; • a fine of KRW 30m for an ICSP who doesn’t comply with a corrective order.	

[140] Above n 1, 371 [112].

#	Question	Response/Yes/No	Comment
	– Arrest – Other	Further, in 2014 the PIPC imposed a KRW212m fine and imposed a corrective order against google to destroy and personal information collected illegally, indicating that large fines and a wide variety of orders can be made against a breaching service provider under either act (as this was before the 2016 amendments).[141] The maximum penalties for data security breaches are: • a fine of KRW 50 million for a data controller who fails to implement the required security measures • a fine of up to KRW 20 million or up to two years imprisonment for a person responsible for a failure to implement required security measures that leads to damage or compromise of personal data • a fine of up to KRW 20 million for a data handler whose legal representative or employee is responsible for a failure to implement required security measures that leads to damage or compromise of personal data • a penalty surcharge of up to KRW 500 million for a data controller who is at fault for the leakage of resident registration numbers it has been processing[142]. There is also criminal liability attached to the provision of personal data without the data subjects consent.[143] Data subjects may also have civil remedies against a service provider.[144]	

[141] Above n 1, 380 [159].
[142] Above n 12.
[143] Above n 1, 350 [29].
[144] Above n 1, 352 [32].

#	Question	Response/Yes/No	Comment
13	Who monitors the correct implementation of the law • Parliament? • Consumer associations / civil society? • Nobody? • Other?	The data protection authorities have enforcement powers. The MOIS, PIPC, Financial Services Commission and Public Prosecutors all have investigatory powers. The PIP Act requires that data breaches be reported to the relevant data protection authorities.	

Europe

Country: European Union

Questionnaire

#	Question	Response/Yes/No	Comment
1	What is the relevant legislation? Are general data protection laws the only relevant laws or are there other sector specific laws as well that may impose additional requirements?	GDPR: horizontal legislation Specific EU legislation for law enforcement authorities ePrivacy Directive (in course of review): sector-specific legislation for confidentiality of communications	Answers below will be based on GDPR unless specified.
2	Are there any bills currently before parliament, or expected to come before parliament, that propose to amend the existing regime?	Yes: ePrivacy Regulation, updating ePrivacy Directive	
3	What type of approach is this? • Consumer protection led?	Horizontal; except ePrivacy Directive which is specific for the electronic communications sector	

#	Question	Response/Yes/No	Comment
	• Other?		
4	What is the scope of the law? • Telecoms? • Social media? • Media? • Medical? • Banking? • Other?	Horizontal; except ePrivacy Directive which is specific for the electronic communications sector; some sector-specific legislations also apply, such as for financial services or healthcare	
5	What does it imply in terms of data collection? • Do all types of data need to be captured, or only personal data? How are they categorised? • Is the data stored by the commercial entity or by a public entity?	Horizontal GDPR: focused on any personal data (this includes pseudonymised personal data); more restrictive rules for sensitive personal data (e.g. health data, religious affiliation etc) Can be stored by any organization: commercial or public No obligation to share/copy/send to a public entity	

#	Question	Response/Yes/No	Comment
	• Is the data copied / sent to a public entity?		
6	What does it imply in terms of data storage? • Does data have to be stored locally? • Can data be stored outside of the country? • Can data stored locally be exported outside of the country? • Does that require an authorisation? • If so, by whom?	No obligation to store locally, but EU safeguards need to be applied when data is transferred out of the EU Yes, can be stored outside the country. Yes, can be stored locally and exported out of the country (subject to specific conditions). Yes, exportation of locally stored data can be subject to authorisation or other mechanisms that prove EU standards are respected. If authorisation is required, it's from the local data protection authorities (in each EU MS).	
7	What does it imply in terms of data processing? • Do the same processes apply to all data, or only to personal data? • Are these processes same for	Only personal data	

#	Question	Response/Yes/No	Comment
	technical and commercial usage? • Can data be processed abroad? If so, does the data processor have to give mirror access locally? • How long is the data stored? • Is the data destructed after that period of time, or kept? • Is that monitored independently, or only by the State?	Yes Yes, data can be processed abroad and need to fulfil all EU requirements and comply with EU law No longer than necessary to fulfil the purpose of the processing Should be deleted, but some exceptions apply Monitoring is done by independent local data protection authorities (in each EU MS)	
8	What does it imply in terms of data usage? • Can data be sold? • Can statistical data be sold? • Can technical data be sold?	Yes, if the conditions of EU law are fulfilled Yes, if the conditions of EU law are fulfilled Yes, if the conditions of EU law are fulfilled	

#	Question	Response/Yes/No	Comment
9	What control do people have on their data? • Are people informed of the data being collected? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) as a bulk? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) line by line? • How is that approval stored? • Who monitors it?	Yes Yes, though some variations apply depending on the type of processing EU law foresees a general documentation obligation for organisations processing personal data, including for consent by people Local independent data protection authorities	
10	Who is responsible for the implementation of the law? • NRA? • Ministry of ICT?	National governments (Ministries)	

#	Question	Response/Yes/No	Comment
	• Army (or affiliate)? • Other?		
11	Who is responsible for possible breaches to the law? • Users? • Service provider? • Local operator? Just for themselves, or also on behalf of their counterparts? • Foreign operator / data handler?	Can be all	
12	Implications of breach • Risks to companies – Penalties – Loss of license – Other • Risks to people	Sanctions include warnings, requests to suspend data operations and fines (up to 4% of worldwide global turnover for a private entity). No criminal sanctions such as arrests or imprisonment.	

#	Question	Response/Yes/No	Comment
	– Penalties – Arrest – Other		
13	Who monitors the correct implementation of the law • Parliament? • Consumer associations / civil society? • Nobody? • Other?	EU Commission Enforcement of the law is done by local independent data protection authorities	

South America

Country: Argentina

Questionnaire

#	Question	Response/Yes/No	Comment
1	What is the relevant legislation? Are general data protection laws the only relevant laws or are there other sector specific laws as well that may impose additional requirements?	Yes.	• In Argentina, personal data protection is governed by Personal Data Protection Law No. 25,326 (“PDPL”), which has the main purposes of guaranteeing (i) the complete protection of the data contained in files, records, databases or other technical means, whether public or private; and (ii) the rights to reputation, privacy, and access to information. • The Do Not Call Law No. 26,951 and complementary regulations. Other sector specific laws such as Telecommunication Law No. 27,078 (Argentina Digital) may impose additional requirements
2	Are there any bills currently before parliament, or expected to come before parliament, that propose to amend the existing regime?	Yes.	In September 2018, a bill intended to completely supersede the DPL was introduced by the Executive Branch in Senate. This bill is inspired on Regulation EU 2016/679 (GDPR). The most relevant developments of the bill are as follows: • broadens the scope of the law and incorporates new definitions;

#	Question	Response/Yes/No	Comment
			• provides that consent may be given expressly, but also—depending on the circumstances—implicitly; • provides that children over 13 years old are authorized to consent to information society services specifically targeted to them; • provides for the data subject's right to data portability and right to be forgotten; • does not require database registration, but incorporates the obligation of keeping records of processing activities and other obligations based on the accountability principle • imposes the obligation of reporting data breaches to the DPA and data subjects; • provides mandatory appointment of a Data Protection Officer (DPO) in connection with public databases, private or public databases treating sensitive data as a main activity, and when undertaking big data processing (the DPA may also request the appointment of a DPO if considered necessary), and • allows international transfer of data among companies of the same economic group (with no need for data subject's consent)
3	What type of approach is this? • Consumer protection led?	• Other	Please refer to our answer to #1 above.

#	Question	Response/Yes/No	Comment
	• Other?		
4	What is the scope of the law? • Telecoms? • Social media? • Media? • Medical? • Banking? • Other?	• Other	Any information related to individuals or companies, whether identified or identifiable, is considered personal data and subject to the terms of the PDPL.
5	What does it imply in terms of data collection? • Do all types of data need to be captured, or only personal data? How are they categorised? • Is the data stored by the commercial entity or by a public entity?	• The PDPL applies to personal data (please see the PDPL's definition above) and sensitive data. Personal data means any kind of information referred to individuals or legal entities. Sensitive data is defined as defined as information pertaining to the Subject's racial or ethnic origin, political opinions, moral, religious or philosophical views, syndicate affiliations, health, or sexual preferences.	N/A

#	Question	Response/Yes/No	Comment
	• Is the data copied / sent to a public entity?	• It applies to all public and private entities. • No.	
6	What does it imply in terms of data storage? • Does data have to be stored locally? • Can data be stored outside of the country? • Can data stored locally be exported outside of the country? • Does that require an authorisation? • If so, by whom?	• No. International transfer of personal data is allowed upon compliance with certain regulatory requirements. • Yes, provided that the regulatory requirements regarding international transfers of personal data are met. • Yes, provided that the regulatory requirements regarding international transfers of personal data are met. • Depending on the case • Data subject	The PDPL sets forth certain restrictions in connection with the international transfer of personal data. Specifically, the PDPL prohibits the cross-border transfer of personal data from Argentina to other countries, if these countries do not provide an adequate level of protection. Disposition 60-E/2016 declared the following countries as providing an adequate level of protection: member states of the European Union and the European Economic Area, Switzerland, Guernsey and Jersey, the Isle of Man, the Faeroe Islands, Canada (only private sector), New Zealand, Andorra, Israel, Great Britain, North Ireland and Uruguay. This white list could be periodically modified by the Argentine Agency of Access to Public Information ("ADPA"). Unfortunately, USA has not been included in the current white list as it has not sanctioned a comprehensive federal law on personal data protection yet. International data transfers to countries not included in ADPA's white list are also permitted when: (i) the data subjects consent to the transfer; or (ii) when adequate protection levels arise from contractual clauses (i.e. international data transfer agreements) or self-regulation systems (i.e. binding corporate rules). ADPA's Rule 60-E/2016 approved two sets of standard model clauses for data controller-data controller transfers as well as data controller-data processor transfers. Parties may freely use these templates or implement a different data transfer agreement as long as this reflect the principles, safeguards and content related to personal data protection provided in the standard model clauses. In the event that the parties opt to use a different model for the data transfer to non-adequate countries that does not reflect the principles, safeguards and content related to personal data protection provided in the standard model clauses, then such agreement will need to be

#	Question	Response/Yes/No	Comment
			submitted to the ADPA for approval within the term of 30 calendar days from its execution.
7	What does it imply in terms of data processing? • Do the same processes apply to all data, or only to personal data? • Are these processes same for technical and commercial usage? • Can data be processed abroad? If so, does the data processor have to give mirror access locally? • How long is the data stored? • Is the data destructed after that period of time, or kept? • Is that monitored independently, or only by the State?	• Only personal data • Yes. • Yes. Mirror access is not necessary, unless required by specific regulations. • Not specifically regulated. Data storage must not exceed the purpose of its collection. • Personal data must be deleted or returned after it ceases to be necessary. • It is monitored independently.	N/A

#	Question	Response/Yes/No	Comment
8	What does it imply in terms of data usage? • Can data be sold? • Can statistical data be sold? • Can technical data be sold?	• No • Yes, provided the data is anonymous • Yes, provided the data is anonymous	Personal data can only be assigned (i) for the compliance of purposes directly related to the legitimate interest of the assignor and assignee and (ii) if made with the previous consent of the Data Subject. Such consent may be revoked. Additionally the Data Subject must be informed of the purpose of the assignment as well as of the identity of the assignee. Consent to the assignment shall not be required in the following cases: - If it is so provided by law. - Where the use of Personal Data is not subject to the Data Subject's consent (see above). - If it is made between governmental agencies pursuant to their legal authority. - When Personal Data is related to the health of subject and its disclosure is necessary for public health reasons. The identity of the individual must be preserved. - If, due to the process used, the Data Subject may not be identified (dissociated information).
9	What control do people have on their data? • Are people informed of the data being collected? • Are people capable of accepting (= they want it) or rejecting (= they	• People must be informed • Yes.	At the point of collection of the personal data, Data Subjects must be informed as to: - The purpose of the collection of the information in question and the potential recipients thereof. - The existence of the data base and the address of the responsible person. - The nature of the questions presented (i.e., whether they are mandatory or optional). - The consequences of the failure to answer or of providing an inaccurate answer to the questions presented.

#	Question	Response/Yes/No	Comment
	don't want it) as a bulk? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) line by line? • How is that approval stored? • Who monitors it?	• Yes. • There is no specific regulation on the storage of the data subject's consents. Each data controller is responsible for monitoring their data processing activities while the authority responsible for controlling compliance with the PDPL is the ADPA.	- The mandatory rights to access, rectification and suppression of the personal data. As a general rule, valid data treatment requires the free, express, informed and written (or similar) consent of the data subject (i.e. the relevant individual or legal entity). Data subjects are free to revoke their consent, although this will only have effects for the future (not retroactively). They also have the right to access to, rectify and suppress their personal data. Treatment of data which is limited to the data subject's name, ID No., Tax ID No., occupation, date of birth and domicile, does not require consent.
10	Who is responsible for the implementation of the law? • NRA? • Ministry of ICT? • Army (or affiliate)? • Other?	ADPA	N/A
11	Who is responsible for possible breaches to the law? • Users?	Data controllers are the main responsible for possible breaches to the law.	N/A

#	Question	Response/Yes/No	Comment
	• Service provider? • Local operator? Just for themselves, or also on behalf of their counterparts? • Foreign operator / data handler?		
12	Implications of breach • Risks to companies – Penalties – Loss of license – Other • Risks to people – Penalties – Arrest – Other	 • Yes • No • Yes • No • Yes • No	Notwithstanding claims from data subjects for damages and liabilities resulting from any non-compliance with the PDPL, the ADPA may apply the following sanctions: (i) warning, (ii) suspension, (iii) fines from AR$ 1,000 to AR$ 100,000 (approx. USD 24 to USD 2400) with a maximum cap of AR$ 5.000.000 (approx. USD 121.000) (iv) closure of the data base or (v) cancellation of the database. The Argentine Criminal Code punishes with imprisonment from one month to three years those who: (i) illegally insert information in a Database; (ii) illegally gain access to Databases; (iii) disclose personal data protected by duty of confidentiality pursuant to law; or (iv) knowingly supply false information stored in a Database to a third party.
13	Who monitors the correct implementation of the law	ADPA	N/A

#	Question	Response/Yes/No	Comment
	• Parliament? • Consumer associations / civil society? • Nobody? • Other?		

Country: Brazil

Questionnaire

#	Question	Response/Yes/No	Comment
1	What is the relevant legislation? Are general data protection laws the only relevant laws or are there other sector specific laws as well that may impose additional requirements?	Brazil has a General Data Protection Law (Law nº 13.709/2018) that will come into force on August 16th 2020, but it also have other specific rules as well as the cyber security policy of financial institutions (Resolution CMN 4,658/2018); the Telecommunication General Law (Law nº 9,472/1997); the Brazilian Civil Rights Framework for the Internet (Law nº 12,965/2014); or the Access to Information Law (Law nº12,527/2011), for example.	Brazil already had a lot of sectorial, dispersed legislation on data protection that still applies, but the General Data Protection Law (LGPD, in Portuguese) rules a broader range of activities and is likely to give the country a greater level of personal data protection.
2	Are there any bills currently before parliament, or expected to come before parliament, that propose to amend the existing regime?	Yes, there is an Executive Order (Nº 869/2018) still on National Congress debate with 176 amendments to be voted.	
3	What type of approach is this? • Consumer protection led? • Other?	The LGPD aims to protect personal data and the privacy of its subjects (it has "the purpose of protecting the essential rights of freedom and privacy and the free development of the personality of the individuals", Article 1)	

#	Question	Response/Yes/No	Comment
4	What is the scope of the law? • Telecoms? • Social media? • Media? • Medical? • Banking? • Other?	The Brazilian General Data Protection Law (LGPD, in Portuguese) is a *General* law, reaching all economic sectors.	It applies to "any processing operation carried out by a natural person or legal entity governed by public or private law, irrespective of the means, of the country in which its headquarter is located or of the country in which the data are located, provided: I- the processing operation be carried out in the Brazilian territory; II – the purpose of the processing activity be the offer or supply of goods or services or the processing of data of individuals located in the Brazilian territory; III – the processed personal data have been collected in the Brazilian territory" (Article 3).
5	What does it imply in terms of data collection? • Do all types of data need to be captured, or only personal data? How are they categorised?	LGPD applies only to the processing of personal data, namely "any operation carried out with personal data, such as those that refer to the collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, information evaluation or control, modification, communication, transfer, diffusion or extraction" (Article 5, X). The personal data is categorized by the law in *personal data,* this is the *"information related to an identified or identifiable a natural person"* and *sensitive personal data* (similar to the "special" category of GDPR), this is, "personal data on racial or ethnic origin, religious belief, public opinion, affiliation to union or religious, philosophical or	

#	Question	Response/Yes/No	Comment
	• Is the data stored by the commercial entity or by a public entity? • Is the data copied / sent to a public entity?	political organization, data relating to the health or sex life, genetic or biometric data, whenever related to a natural person" (Article 5, I and II). The data is not stored, copied or sent to any commercial or public entity. However, the processing must comply with the Law and there may be inspections about it by the National Data Protection Authority.	
6	What does it imply in terms of data storage? • Does data have to be stored locally? • Can data be stored outside of the country? • Can data stored locally be exported outside of the country? • Does that require an authorisation? • If so, by whom?	The data could be stored and transferred anywhere with an appropriate level of protection; where the controller provides and demonstrates guarantees of compliance with the principles, rights of the data subject and data protection regime established in this Law, in the form of: a) specific contractual sections for a given transfer; b) standard contractual sections; c) global corporate rules; d) seals, certificates and codes of conduct regularly issued; where the transfer is required for international legal cooperation between government intelligence, investigation and police bodies, in accordance with the international law instruments; where the transfer is required for life protection or physical integrity of the data subject or any third party; where the supervisory authority authorizes such transfer; where the transfer results in a commitment undertaken under an international cooperation agreement; where the transfer is required for enforcement of a public policy or legal attribution of the public utility; where the data subject has provided specific and highlighted consent for such transfer, with previous information on the international nature of the operation, clearly distinguishing it from any other purposes; or where required to compliance with a statutory or regulatory obligation by the controller; the performance of agreements or preliminary procedures relating to agreements to which the data subject is a party, at the request of the data subject and the regular exercise of rights in lawsuits, administrative or arbitration proceedings (Article 33).	
7	What does it imply in terms of data processing? • Do the same processes apply to	This applies to all personal data – including personal data processing for technical and commercial usage. The only exception in this matter (which means, in these cases LGPD does not apply) are in the Article 4: "processing of personal data: I – made by a natural person for exclusively private and non-economic purposes; II – made exclusively for: a) journalistic and artistic purposes; or b) academic purposes,	

#	Question	Response/Yes/No	Comment
	all data, or only to personal data? • Are these processes same for technical and commercial usage? • Can data be processed abroad? If so, does the data processor have to give mirror access locally? • How long is the data stored? • Is the data destructed after that period of time, or kept? • Is that monitored independently, or only by the State?	in which case articles 7 and 11 of this Law shall apply; III - made exclusively for the following purposes: a) public security; b) national defense; c) safety of the Country; or d) crime investigation and punishment activities; or IV – originating from outside the Brazilian territory and which are not subject to communication, shared use of data with Brazilian processing agents or subject to international transfer of data with other country than the country of origin, provided the country of origin provides a degree of personal data protection consistent with the provisions of this Law." The data could be processed abroad without the obligation to give mirror access locally. In short, data must be destructed if there isn´t any legal basis (Article 7) for processing it. Yet, in detail, Article 15 dictates that the "termination of the processing of personal data shall occur in the following events: I – verification that the purpose was reached or that the data are no longer necessary or pertinent to attain the specific purpose sought; II – lapse of the processing period; III - communication of the data subjects, including in the exercise of their right to revoke the consent as set forth in paragraph 5 of article 8 of this Law, upon protection of the public interest; or IV – order of the supervisory authority, in the event of breach of the provisions of this Law." It will be monitored by the Brazilian Nacional Data Protection Authority, which is currently related to the Presidency of the Republic (Article 55-A).	
8	What does it imply in terms of data usage? • Can data be sold? • Can statistical data be sold?	Brazil has a General Data Protection Law (Law nº 13.709/2018) that will come into force on August 16th 2020, but it also have other specific rules as well as the cyber security policy of financial institutions (Resolution CMN 4,658/2018); the Telecommunication General Law (Law nº 9,472/1997); the Brazilian Civil Rights Framework for the Internet (Law nº 12,965/2014); or the Access to Information Law (Law nº12,527/2011), for example.	Brazil already had a lot of sectorial, dispersed legislation on data protection that still applies, but the General Data Protection Law (LGPD, in Portuguese) rules a broader range of activities

#	Question	Response/Yes/No	Comment
	• Can technical data be sold?		and is likely to give the country a greater level of personal data protection.
9	What control do people have on their data? • Are people informed of the data being collected? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) as a bulk? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) line by line? • How is that approval stored? • Who monitors it?	Yes, there is an Executive Order (Nº 869/2018) still on National Congress debate with 176 amendments to be voted.	

#	Question	Response/Yes/No	Comment
10	Who is responsible for the implementation of the law? • NRA? • Ministry of ICT? • Army (or affiliate)? • Other?	The LGPD aims to protect personal data and the privacy of its subjects (it has "the purpose of protecting the essential rights of freedom and privacy and the free development of the personality of the individuals", Article 1)	
11	Who is responsible for possible breaches to the law? • Users? • Service provider? • Local operator? Just for themselves, or also on behalf of their counterparts? • Foreign operator / data handler?	The Brazilian General Data Protection Law (LGPD, in Portuguese) is a *General* law, reaching all economic sectors.	It applies to "any processing operation carried out by a natural person or legal entity governed by public or private law, irrespective of the means, of the country in which its headquarter is located or of the country in which the data are located, provided: I- the processing operation be carried out in the Brazilian territory; II – the purpose of the processing activity be the offer or supply of goods or services or the processing of data of individuals located in the Brazilian territory; III – the processed personal data have been

#	Question	Response/Yes/No	Comment
			collected in the Brazilian territory" (Article 3).
12	Implications of breach • Risks to companies – Penalties – Loss of license – Other • Risks to people – Penalties – Arrest – Other	LGPD applies only to the processing of personal data, namely "any operation carried out with personal data, such as those that refer to the collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, information evaluation or control, modification, communication, transfer, diffusion or extraction" (Article 5, X). The personal data is categorized by the law in *personal data,* this is the *"information related to an identified or identifiable a natural person"* and *sensitive personal data* (similar to the "special" category of GDPR), this is, "personal data on racial or ethnic origin, religious belief, public opinion, affiliation to union or religious, philosophical or political organization, data relating to the health or sex life, genetic or biometric data, whenever related to a natural person" (Article 5, I and II). The data isn´t stored, copied or sent to any commercial or public entity. However, the processing must comply with the Law and there may be inspections about it by the National Data Protection Authority.	
13	Who monitors the correct implementation of the law • Parliament? • Consumer associations / civil society? • Nobody?	The data could be stored and transferred anywhere with an appropriate level of protection; where the controller provides and demonstrates guarantees of compliance with the principles, rights of the data subject and data protection regime established in this Law, in the form of: a) specific contractual sections for a given transfer; b) standard contractual sections; c) global corporate rules; d) seals, certificates and codes of conduct regularly issued; where the transfer is required for international legal cooperation between government intelligence, investigation and police bodies, in accordance with the international law instruments; where the transfer is required for life protection or physical integrity of the data subject or any third party; where the supervisory authority authorizes such transfer; where the transfer results in a commitment undertaken under an international cooperation agreement; where the transfer is required for enforcement of a public policy or legal attribution of the public utility; where the data subject has provided specific and	

#	Question	Response/Yes/No	Comment
	• Other?	highlighted consent for such transfer, with previous information on the international nature of the operation, clearly distinguishing it from any other purposes; or where required to compliance with a statutory or regulatory obligation by the controller; the performance of agreements or preliminary procedures relating to agreements to which the data subject is a party, at the request of the data subject and the regular exercise of rights in lawsuits, administrative or arbitration proceedings (Article 33).	

Country: Chile

Questionnaire

#	Question	Response/Yes/No	Comment
1	What is the relevant legislation? Are general data protection laws the only relevant laws or are there other sector specific laws as well that may impose additional requirements?	The statute that governs data protection and privacy law issues in Chile is contained in Law N° 19,628 on Personal Data and Privacy (hereinafter, the "Law"). For some specific data, there are some other laws or regulations may result applicable, such as Consumers' Protection Law (regulating the spam), Labour Law and other Labour Regulation (regulating the protection of employees' privacy and e-mails) and Banking Regulations (regulating bank secrecy and bank reserve).	
2	Are there any bills currently before parliament, or expected to come before parliament, that propose to amend the existing regime?	Yes. The Chilean Congress is currently discussing and processing a bill that will substantially modify the Law.	
3	What type of approach is this? • Consumer protection led? • Other?	The Law was originally drafted with the idea of regulating the data collection activity, especially those issues concerning the gathering and management of personal data. The application of the Law affects any type of data collectors, including companies dealing with their employees' personal data, even though it was not originally the main objective of the law. The approach is mainly individual´s protection.	
4	What is the scope of the law?	Any person, in any type of industry, who gathers, manages and processes personal data.	

#	Question	Response/Yes/No	Comment
	• Telecoms? • Social media? • Media? • Medical? • Banking? • Other?		
5	What does it imply in terms of data collection? • Do all types of data need to be captured, or only personal data? How are they categorised? • Is the data stored by the commercial entity or by a public entity? • Is the data copied / sent to a public entity?	• It will depend on what is the collector looking for by the collection. The Law defines "*personal data*" as any information concerning an identified individual; and defines "*sensible data*" as personal information related with the physical and moral characteristics of the individual, facts or circumstances of his/her private life, such as personal habits, racial origin, ideas or political opinions, religion, physical and physiological health and sexual life. • The data may be store either by a private or public entity. • No, data is not copied or sent to a public entity, unless the public entity requests this information and is empowered to do so.	
6	What does it imply in terms of data storage?	• The Law does not address this matter, but according to the *Instituto Chileno de Derecho y Tecnologías, a* Chilean non-profit private law corporation, composed mainly by university professors and highly specialized	

#	Question	Response/Yes/No	Comment
	• Does data have to be stored locally? • Can data be stored outside of the country? • Can data stored locally be exported outside of the country? • Does that require an authorisation? • If so, by whom?	professionals (hereinafter, the "Instituto"), in a broad interpretation of the Chilean Constitution and the Law, whoever has personal data is legally responsible for them, therefore must take the necessary measures to store them in a secure environment, regardless of country or locality. • The Law does not address this matter, but according to the Instituto in a broad interpretation of the Constitution and the Law, the data can be stored outside the country, however this must be encrypted. • The Law only refers to the transmission of personal data to international organizations, which has to be in compliance with the provisions of the treaties and agreements in force. As the Law does not address other situations, in a broad interpretation of the Constitution and the Law, the data can be exported outside the country, as long as it complies with other aspects of the Law (as the express written consent of the of the individuals whose personal information is collected, hereinafter the "data subjects" and the use of the data only for the purposes for which it was collected). • The Law does not address this matter, but at least, the data subjects must have given their express written consent for the collection of their data. • The Law does not address this matter.	
7	What does it imply in terms of data processing? • Do the same processes apply to all data, or only to personal data? • Are these processes same for	• Only to personal data, as the Law defines Data processing, as any operation or complex of operations or technical procedures, of automated character or not, that allow to collect, store, record, organize, elaborate, select, extract, confront, interconnect, dissociate, communicate, assign, transfer, transmit or cancel personal data, or use them in any other way. • The Law does not make a distinction regarding the processes for technical and commercial usage.	

#	Question	Response/Yes/No	Comment
	technical and commercial usage? • Can data be processed abroad? If so, does the data processor have to give mirror access locally? • How long is the data stored? • Is the data destructed after that period of time, or kept? • Is that monitored independently, or only by the State?	• The Law does not address this matter. • The Law does not address this matter. • The Law does not address this matter. • Independently.	
8	What does it imply in terms of data usage? • Can data be sold? • Can statistical data be sold? • Can technical data be sold?	• The Law does not address this matter, but we may infer that, unless the data subject has given his/her consent for the sale of the data, these information cannot be sold. • The Law does not address this matter, but we may infer that, unless statistical data has personal or sensitive data, it can be sold. • The Law does not address this matter, but we may infer that, unless technical data has personal or sensitive data, it can be sold.	

#	Question	Response/Yes/No	Comment
9	What control do people have on their data? • Are people informed of the data being collected? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) as a bulk? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) line by line? • How is that approval stored? • Who monitors it?	• In practice, sometimes. However, the Law states a specific element in relation to this matter, which is the recognition and acceptance of an individual's prior written approval for the gathering and management of his/her personal data. This prior, written and express consent is also a requisite for the gathering and management of sensible data. The Law states that, as a general rule, "personal data management may be conducted only when the law or other regulations authorize it or the data subject expressly consents. The data subject must be duly informed about the purpose of his/her personal data gathering, storage and its possible public disclosure. Therefore, it can be inferred that a prior, written, and express consent of the affected individual is mandatory when the law or other regulations does not authorize his/her personal data gathering and management. However, the Law also contains several exemptions to the general rule. • The Law does not address this matter. In practice, the most usual way of informing people that their data is being collected, is by giving the option to accept/refuse the Terms and Conditions/Privacy Policies of the entity that is collecting the information (i.e. When downloading an app, it is usually mandatory to accept the Terms and Conditions/Privacy Policies). • The Law does not address this matter, but in practice, no. • The Law does not address this matter. • The data collectors.	
10	Who is responsible for the implementation of the law? • NRA? • Ministry of ICT?	No specific governmental entity, just the data collectors.	

#	Question	Response/Yes/No	Comment
	• Army (or affiliate)? • Other?		
11	Who is responsible for possible breaches to the law? • Users? • Service provider? • Local operator? Just for themselves, or also on behalf of their counterparts? • Foreign operator / data handler?	The owner of a database where personal data is stored after its collection shall be responsible to employ due care in its maintenance and shall be liable for the damages. The owner of a database containing personal data shall be liable to indemnify the actual pecuniary damages and the moral damages caused by its improper processing of the data, without prejudice of eliminating, modifying or blocking the data as requested by the data subject or upon a court order, in its case. The legal action to pursue this action for damages shall be subject to summary action procedures. The judge in light of the circumstances and the gravity of the facts shall prudentially determine the amount of the damages that can be awarded by the court.	
12	Implications of breach • Risks to companies – Penalties – Loss of license – Other • Risks to people	The Law states that the implications of breaching the Law is the compensation of the patrimonial and moral damage caused (monetary fines).	

#	Question	Response/Yes/No	Comment
	– Penalties – Arrest – Other		
13	Who monitors the correct implementation of the law • Parliament? • Consumer associations / civil society? • Nobody? • Other?	No specific entity monitors the correct implementation of the Law. The bill that currently is in the Chilean Congress seeks to amend this by creating an Agency for the Protection of Personal Data.	

Country: Colombia

Questionnaire

#	Question	Response/Yes/No	Comment
1	What is the relevant legislation? Are general data protection laws the only relevant laws or are there other sector specific laws as well that may impose additional requirements?	Fundamental right: Article 15 of the Colombian Constitution establishes habeas data as a fundamental right. General data protection laws: Law 1581 of 2012 and Decree 1074 of 2015, provide the general framework of data privacy regulations. Criminal offences: Law 1273 of 2009 establishes criminal offences concerning data privacy. Sector-specific for financial personal data: Law 1266 of 2008 and Decree 1729 of 2009.	
2	Are there any bills currently before parliament, or expected to come before parliament, that propose to amend the existing regime?	No.	
3	What type of approach is this? • Consumer protection led? • Other?	Consumer protection led.	

#	Question	Response/Yes/No	Comment
4	What is the scope of the law? • Telecoms? • Social media? • Media? • Medical? • Banking? • Other?	All. The law covers the processing of any kind of information that may lead to the identification of an individual.	
5	What does it imply in terms of data collection? • Do all types of data need to be captured, or only personal data? How are they categorised? • Is the data stored by the commercial entity or by a public entity? • Is the data copied / sent to a public entity?	Data protection regulation covers only personal data. A special category of “personal data” is “sensitive personal data”, which are data which might lead to discrimination against the data subject. No service or activity can be conditional on the processing of sensitive personal data. Data protection regulations apply to both commercial and public entities (understood as government agencies and not as public companies as in US Law). Personal data is not required to be copied or sent to public entities.	

#	Question	Response/Yes/No	Comment
6	What does it imply in terms of data storage? • Does data have to be stored locally? • Can data be stored outside of the country? • Can data stored locally be exported outside of the country? • Does that require an authorisation? • If so, by whom?	Any kind of data storage is covered by data protection regulation. Data can be stored locally by data processors or data controllers. Data processors should comply with the data controller's privacy policies, and should process data with high degrees of security and confidentiality. Data can be stored outside Colombia whenever (i) data subjects expressly authorized such processing; (ii) data controller signs a data transfer agreement with the data processor establishing the scope of the processing activities, confidentiality obligations, and safekeeping obligations; or (iii) the Data Protection Authority (the Superintendence of Industry and Commerce) issued a statement of conformity authorizing the processing of personal data abroad. Personal data can be transferred to another data controller outside Colombia whenever (i) Data subjects expressly authorized the recipient country; (ii) the Data Protection Authority considers that the recipient country grants similar levels of personal data protection; (iii) the Data Protection Authority issued a statement of conformity authorizing the transfer of personal data abroad; or (iv) the parties notified to the Data Protection Authority a data transfer agreement in which confidentiality and safekeeping obligations were established.	
7	What does it imply in terms of data processing? • Do the same processes apply to all data, or only to personal data? • Are these processes same for technical and commercial usage?	These processes apply to personal data. They are the same regardless of the purpose of the processing. Data can be transferred abroad, without any third party needing to give mirror access locally. Personal data cannot be processed after the purposes for which data subjects consented its processing are met, and has to be destroyed, unless there is a legal or judicial mandate that requires the personal data to be kept. The authority in charge of monitoring compliance with data protection regulation is the Superintendence of Industry and Commerce.	

#	Question	Response/Yes/No	Comment
	• Can data be processed abroad? If so, does the data processor have to give mirror access locally? • How long is the data stored? • Is the data destructed after that period of time, or kept? • Is that monitored independently, or only by the State?		
8	What does it imply in terms of data usage? • Can data be sold? • Can statistical data be sold? • Can technical data be sold?	For personal data to be sold, prior consent from data subjects is required. Statistical Data is not considered personal data if it does not allow for the identification of data subjects.	
9	What control do people have on their data?	Except in the cases expressly provided for in CDPR, personal data may not be collected without subjects' consent. Data controllers should require data subjects' consent before processing their personal data.	Data subjects have the following rights:

#	Question	Response/Yes/No	Comment
	• Are people informed of the data being collected? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) as a bulk? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) line by line? • How is that approval stored? • Who monitors it?	Said consent should be granted through means that may be subject to further consultation. Silence may never be understood as consent. Consent forms should explain what treatment will personal data be given, what purposes it will be processed for, what the data subjects' rights are, and how to contact the data controller. Unless sensitive personal data are to be processed, people are capable of accepting or rejecting as a bulk. The authority in charge of monitoring compliance with data protection regulation is the Superintendence of Industry and Commerce.	• Get to know, update and correct his/ her Personal Data. • Request proof of the granted consent. • Be informed, having requested it, with respect to the use of his/ her Personal Data. • Present complaints before the Superintendence of Industry and Commerce due to violations of Colombian data protection regulation. • Request the Personal Data to be suppressed (opt-out). Notice that the latter entails that both data controllers and data processors should allow for opt-out mechanisms for data subjects. Such mechanisms should be publicly

#	Question	Response/Yes/No	Comment
			announced (e.g. in the privacy policy). • Revoke his/ her consent by presenting a request and/ or claim. This does not proceed when the data subject has a legal or contractual duty to remain in the database (e.g. where there is an employment contract). • Request the Superintendence of Industry and Commerce to order the consent to be revoked and/ or the Personal Data to be suppressed. • Freely consult his/ her Personal Data at least once every calendar month and every time the Data Processing Policies are substantially modified.

#	Question	Response/Yes/No	Comment
10	Who is responsible for the implementation of the law? • NRA? • Ministry of ICT? • Army (or affiliate)? • Other?	The Superintendence of Industry and Commerce oversees the implementation of data protection regulation.	
11	Who is responsible for possible breaches to the law? • Users? • Service provider? • Local operator? Just for themselves, or also on behalf of their counterparts? • Foreign operator / data handler?	Data controllers and data processors are both responsible for possible breaches to data protection regulation.	

#	Question	Response/Yes/No	Comment
12	Implications of breach • Risks to companies – Penalties – Loss of license – Other • Risks to people – Penalties – Arrest – Other	Data protection regulation contemplates the following penalties for breaching this regulation: • Fines of up to 2000 minimum wages (approximately US$500.000); • Orders to suspend data processing activities for up to 6 months, if there are serious security concerns; • Orders to cease data processing activities, in case the undertaking has not modified its data processing structure during the 6-month suspension that was mentioned on point 2; • Orders to cease the processing of sensitive data.	
13	Who monitors the correct implementation of the law • Parliament? • Consumer associations / civil society? • Nobody? • Other?	The Superintendence of Industry and Commerce.	

Country: Mexico

Questionnaire

#	Question	Response/Yes/No	Comment
1	What is the relevant legislation? Are general data protection laws the only relevant laws or are there other sector specific laws as well that may impose additional requirements?	The laws in Mexico that regulate data protection (hereinafter the "Data Protection Laws") are: • Federal Law on Protection of Personal Data in Possession of Private Entities (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* the "DPL")) and its Regulation; and • Federal Law on the Protection of Personal Data in Possession of Regulated Entities (*Ley General de Protección de Datos Personales en Posesión. de Sujetos Obligados*). However, the National Institute on Transparency, Access to Information and Personal Data Protection (*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*, hereinafter "INAI") – the Federal authority in charge of overseeing the due observance of Data Protection Laws in Mexico– can issue interpretation criteria, which are binding for the Obligated Subjects at the federal level and orienting for the local protection agencies. An interpretation criterion is the analysis and report carried out by INAI on a particular subject regarding the protection of personal data or the right of access to information when a relevant issue is identified as a result of legal claims filed by individuals in connection with the violation of such human rights. Consumer Protection legislation mas also apply to data privacy matters in Mexico.	Obligated Subjects are any authority, entity, organ or body of the Executive, Legislative and Judicial Branches of the Mexican Government, autonomous bodies, political parties, trusts and public funds, all of whom must publicly disclose their actions and justify them, being responsible to those affected by their decisions, and are therefore accountable.
2	Are there any bills currently before parliament, or expected to come before parliament,	On February 7, 2019, a bill for the Regulations on Transparency and Access to Public Information and Personal Data Protection for the Senators Chamber came before the same parliament.	The bill does not propose to amend the existing regime, but to include the Senators Chamber as an Obligated Subject in transparency and data protection

#	Question	Response/Yes/No	Comment
	that propose to amend the existing regime?		matters. This Regulations bill seeks to systematize (i) the Senators Chamber's obligations and responsibilities in accordance with the previous related regulations, (ii) the functioning of the governmental entities responsible for transparency and access to information, (iii) the procedures for access to public information, (iv) classified information, (v) the procedure for some appeal proceedings and (vi) its sanctions.
3	What type of approach is this? • Consumer protection led? • Other?	Other.	To include the Senators Chamber as an Obligated Subject in transparency and data protection matters, and systematize its obligations and responsibilities in accordance with the previous related regulations.
4	What is the scope of the law?	The Data Protection Laws aim to protect personal data held by individuals and Obligated Subjects, in order to regulate their legitimate, controlled and informed	The scope of the DPL include all processing of personal data when: (i) it is carried out in an

#	Question	Response/Yes/No	Comment
	• Telecoms? • Social media? • Media? • Medical? • Banking? • Other?	treatment, to ensure the privacy and the right to self-determination information of all individuals.	establishment of the data controller located in Mexico; (ii) it is carried out by a data processor, regardless of its location, on behalf of a data controller established in Mexico; (iii) the data controller is not established in Mexico but is subject to Mexican laws as a consequence of entering into a contract or under international law; and (iv) the data controller or data processor use media located in Mexico.
5	What does it imply in terms of data collection? • Do all types of data need to be captured, or only personal data? How are they categorised? • Is the data stored by the commercial entity or by a public entity?	The Data Protection Laws imply only the personal collection. Categories of personal data: • Identification data. Data that permits the differentiation of individuals. • Contact information. Data that permits the contact of the data controller with the data subject. • Employment data. Data concerning the employment records, position or commission; work performance and professional experience of an individual. • Physical characteristics data. Data related to an individual's physiognomy, anatomy, specific physical particularities.	Pursuant to the Data Protection Laws, personal data is understood as any information concerning an identified or identifiable individual.

#	Question	Response/Yes/No	Comment
	• Is the data copied / sent to a public entity?	• Academic data. Data concerning the academic preparation, skills, and professional or technical development of an individual. • Patrimonial or financial data. Data concerning assets, rights, charges or obligations of an individual subject to economic valuation. • Biometric data. Data regarding the image of the iris, fingerprint, palm of the hand or similar of an individual. • Sensitive data: Data that affects the most intimate sphere of its Data Subject, or the misuse of which may give rise to discrimination or entail a serious risk to it is considered sensitive personal data, such as racial or ethnic origin, present and future health status, genetic information, religious, philosophical and moral beliefs, union affiliation, political opinions, and sexual preference. The personal data can be stored by a commercial or public entity, each of them is regulated on an specific Data Protection Law: • Commercial entity / Private entity: Federal Law on Protection of Personal Data in Possession of Private Entities (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*) and its Regulation; and • Public entity: Federal Law on the Protection of Personal Data in Possession of Regulated Entities (*Ley General de Protección de Datos Personales en Posesión. de Sujetos Obligados*).	
6	What does it imply in terms of data storage? • Does data have to be stored locally? • Can data be stored outside of the country?	According to the Data Protection Laws, personal data (i) can be stored locally and outside the country and (ii) can be exported/transferred outside the country. The express consent (authorization) from data subjects to process their data (including transfer) will be required if the data controller collects and processes financial personal data or sensitive personal. Otherwise, implied consent (i.e. that the privacy notice is made available to data subjects and they do not object to the processing of their personal data) will suffice.	N/A

#	Question	Response/Yes/No	Comment
	• Can data stored locally be exported outside of the country? • Does that require an authorisation? • If so, by whom?		
7	What does it imply in terms of data processing? • Do the same processes apply to all data, or only to personal data? • Are these processes same for technical and commercial usage? • Can data be processed abroad? If so, does the data processor have to give mirror access locally? • How long is the data stored? • Is the data destructed after	The Data Protection Laws only regulate the processing of personal data. If the personal data will be used for commercial or marketing purposes, the privacy notice furnished to the relevant Data Subject shall specifically indicate so. According to the Data Protection Laws, personal data can be processed in Mexico or abroad, without the need to comply with additional requirements. Data Controllers and Obligated Subjects should maintain personal data accurate and up to date. Also, they are required to eliminate data when it is no longer necessary for the purposes specified in the privacy notices delivered to the Data Subjects. The INAI is the only authority in Mexico entitled to oversee and monitor the due observance of Data Protection Laws in Mexico.	Any person that processes (i.e. including collection, storage, transfer, and use) personal data, will act as Data Controller and shall furnish a privacy notice to every individual from whom it processes personal data, which shall at least indicate i) the Data Controller's name and address; ii) the personal data that will be collected and processed; iii) the purposes for which the personal data was gathered; iv) The mechanisms through which Data Subjects may (a) exercise their rights (so called ARCO Rights, (b) limit the use or disclosure of their personal data; and (c) revoke their consent as to the use of their data; v) whether the personal data

#	Question	Response/Yes/No	Comment
	that period of time, or kept? • Is that monitored independently, or only by the State?		will be transferred to third parties and, if applicable, detail the transfers that will be conducted; and vi) the means through which the Data Controller will inform Data Subjects of any changes to the privacy notice.
8	What does it imply in terms of data usage? • Can data be sold? • Can statistical data be sold? • Can technical data be sold?	Data Controllers can only use the personal data for the purposes outlined in the privacy notice. If the data controller will transfer personal data to third parties, the privacy notice must expressly indicate so, as well as the purposes of transferring such personal data. Therefore, if the transfer for such purpose is indicated in the privacy notice that has been consented by the relevant Data Subject, the sell of personal data might be conducted. If the Data Controller intends to use or transfer the data for different purposes than the ones outlined in the privacy notice, renewed consent from the relevant Data Subject will be required.	Data Controllers must obtain the consent of Data Subjects in order to process their personal data; depending on the type of data, the consent required may be express (opt-in) or implied (opt-out), financial or wealth-related data require express consent.
9	What control do people have on their data? • Are people informed of the data being collected? • Are people capable of accepting (= they want it) or rejecting (= they	Data Subjects shall be informed of the personal data that will be collected and processed through the privacy notice. Data Subject shall implicitly and expressly consent the processing of their personal data through the consenting of the privacy notice. Data Subjects may oppose to the use of specific data and / or its use for specific purposes, through the exercise of their ARCO rights. However, Data Controllers will not be obligated to cancel/delete such personal data when, among others, the relevant Data Subject is a party to an agreement and the processing of his/her information is necessary for its performance or enforcement.	Data Subjects in Mexico are entitled to the exercise of ARCO Rights, which consist of: (i) the right to access their data; (ii) the right to rectify their data when inaccurate or incomplete; (iii) the right to cancel or delete their data (especially when it is not required for the purposes outlined in the privacy

#	Question	Response/Yes/No	Comment
	don't want it) as a bulk? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) line by line? • How is that approval stored? • Who monitors it?	Although Data Controllers must implement administrative, physical and technical security measures to protect personal data against loss, theft or unauthorized use, there are no specific indications in the DPL as to the ways through which approval shall be stored. INAI and the corresponding Privacy Officers.	notice); and (iv) the right to oppose to the use of their data for specific purposes (e.g., for marketing purposes). Businesses must appoint a person or department who will address the ARCO rights petitions submitted by Data Subjects, and promote the protection of personal data within the organization ("Privacy Officers").
10	Who is responsible for the implementation of the law? • NRA? • Ministry of ICT? • Army (or affiliate)? • Other?	The INAI.	N/A
11	Who is responsible for possible breaches to the law? • Users?	The DPL imposes obligations on all Data Controllers that process personal data, regardless if they are business or individuals, and is applicable to any Processing of personal data when: (i) such Processing is carried out in an establishment of a data controller located in Mexico; (ii) such Processing is carried out by a data processor (regardless of its location) on behalf of a data controller located in Mexico; (iii) the data controller is not located in Mexico but is bound by Mexican law as a result of an agreement or pursuant to international law; or (iv) the data controller is not	N/A

#	Question	Response/Yes/No	Comment
	• Service provider? • Local operator? Just for themselves, or also on behalf of their counterparts? • Foreign operator / data handler?	located in Mexico but uses means located in such territory, unless such means are used solely for the purposes of mere transit.	
12	Implications of breach • Risks to companies – Penalties – Loss of license – Other • Risks to people – Penalties – Arrest – Other	Failure to comply with the DPL provisions may trigger (a) claims from Data Subjects; (b) investigations conducted by the INAI, which could lead to the imposition of an economic sanction that may range from $442 to $1,415,539 dollars, approximately (amount that can be duplicated when concerning sensitive personal data).	N/A
13	Who monitors the correct implementation of the law	The INAI.	N/A

#	Question	Response/Yes/No	Comment
	• Parliament? • Consumer associations / civil society? • Nobody? • Other?		

Country: Perú

Questionnaire

#	Question	Response/Yes/No	Comments
1	What is the relevant legislation? Are general data protection laws the only relevant laws or are there other sector specific laws as well that may impose additional requirements?	Yes.	Law No. 29733 (Personal Data Protection Law), and its Regulations, approved by Supreme Decree No. 003-2013-JUS are the main legal instruments regarding data protection. However, the Peruvian Constitution, Civil Code and Criminal Code also regulate, in a general way, the right of individuals to their privacy. Other sector specific laws that may impose certain obligations on data processing are the consumer laws and health laws on clinic histories.
2	Are there any bills currently before parliament, or expected to come before parliament, that propose to amend the existing regime?	Yes.	Bill No. 1828/2017-CR seeks to amend Article 18 of Law No. 29733, which currently says that databank controllers who outsource the data processing after the data subjects have provided their consent, must provide a customized communication to all data subjects. According to the aforementioned bill, this could lead to the increase of costs, which will eventually be transferred to the clients. In order to reduce this cost, this bill proposes that databank controllers should be able to adopt efficient mechanisms to communicate any outsourcing of data processing (e.g. announcement in physical, virtual or other similar media), rather than customized communications
3	What type of approach is this?	Other.	This is an omnibus law that regulates all data processing of personal data (contained or destined to be contained in a public or private personal database) equally.

#	Question	Response/Yes/No	Comments
	• Consumer protection led? • Other?		
4	What is the scope of the law? • Telecoms? • Social media? • Media? • Medical? • Banking? • Other?	Other.	As already explained, this is an omnibus law that treats all personal data equally.
5	What does it imply in terms of data collection? • Do all types of data need to be captured, or only personal data? How are they categorised? • Is the data stored by the commercial	• No. • It depends.	• The Data Protection Law only applies to personal data, which is defined as all numerical, alphabetical, graphic, photographic, sound, or any other type of information concerning an individual which identifies or could be used to identify the individual through reasonable means. • According to the Data Protection Law, personal data can be stored by individuals, private legal entities or public entities ("Data controller"), depending on who is in charge of processing the data.

#	Question	Response/Yes/No	Comments
	entity or by a public entity? • Is the data copied / sent to a public entity?	• No.	Data stored by private entities does not need to be copied or sent to a public entity. However, the Data controllers must register their databases containing personal data and report any cross-border transfers of personal data before the Data Protection Authority, by filing the applicable form.
6	What does it imply in terms of data storage? • Does data have to be stored locally? • Can data be stored outside of the country? • Can data stored locally be exported outside of the country? • Does that require an authorisation? • If so, by whom?	• No. • Yes. • Yes. • Yes.	• The Data Protection Law also applies to personal data processed overseas provided that the data controller is established in Peru. • If the data has been stored locally, a cross border transfer may be carried out, provided that the requirements set forth in the following paragraph are met. • Cross border transfers can be carried out, provided that the data subjects provide their consent and that the destination country provides adequate protection for personal data. If the destination country fails to provide adequate protection levels, the exporters must either refrain from making cross-border transfers of personal data, or guarantee that the treatment of personal data meets adequate protection levels (e.g. contractual clauses). This does not apply when, among other cases (a) the data subject has given his or her prior, informed, express and unequivocal consent to the transfer of data under such circumstances; or (b) the cross-border transfer of personal data is needed for the performance of a contractual relationship in which the data subject is a party.

#	Question	Response/Yes/No	Comments
			• In order to carry out cross-border transfers, the data subject's consent is required. Finally, even if no additional authorizations are required, cross border transfers must be reported to the Data Protection Authority by filing the applicable form.

7	What does it imply in terms of data processing?
	• Do the same processes apply to all data, or only to personal data?
	• Are these processes same for technical and commercial usage?
	• Can data be processed abroad? If so, does the data processor have to give mirror access locally?
	• How long is the data stored?
	• Is the data destructed after that period of time, or kept?
		• No.
		• Yes.
		• Yes.
			• The Data Protection Law only applies to personal data.
			• However, consent is not required to process the data when, among others: (i) the data is contained or destined to be contained in a publicly available source (ii) the data is necessary for a contractual, scientific or professional relationship with the data subject, provided that such data is necessary for the development, entering into and compliance with such relationship, (iii) the data is dissociated or anonymized, and (iv) the data is necessary to safeguard the legitimate interest of the data subject, among others.
			• Personal data can be processed abroad, in accordance with any applicable law. However, if Peru's data protection laws are applicable, the following must be taken into account:
			  • For the data to be processed abroad, the data subject's consent will be required.
			  • Any cross border transfer would have to be carried out in accordance to the Data Protection Law.
			  • The data subjects must be duly informed about the purpose of the data collection, the data recipients, the data banks where the data will be stored (including the identity and address of the data bank holder and the people in charge of processing the data), about any

#	Question	Response/Yes/No	Comments
	• Is that monitored independently, or only by the State?		data transfer, the time during which the data will be kept, among others. • According to the Data Protection Law, data subjects have the right to access all their information that is processed and stored in data banks. Therefore, even if there is no express requirement to have a mirror access locally, it will be mandatory to provide this information to the data subjects on a local basis. • Data can be stored during the time it is necessary or pertinent to the purpose for which it was collected, or until the term agreed for its treatment. • The data must be destructed after that period, unless an anonymization or dissociation procedure is used. Besides being monitored by the Data Protection Authority, the data subjects could also monitor and oppose to any unauthorized data treatment or collection.
8	What does it imply in terms of data usage? • Can data be sold? • Can statistical data be sold? • Can technical data be sold?	• Yes.	This has not been expressly regulated by law. However, since it has not been forbidden, we consider that data could be sold, provided that there is an express consent from the data subject. According to the Regulations of the Data Protection Law, gifts could be offered upon the granting of consent, without this meaning that the data subject was not free to grant his/her consent (except for the consent of underage people, when accepted).

#	Question	Response/Yes/No	Comments
9	What control do people have on their data? • Are people informed of the data being collected? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) as a bulk? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) line by line? • How is that approval stored? • Who monitors it?	• Yes. • Yes. • Yes.	• As explained in question 7, data subjects have the right to be informed, before their data is collected, about the purpose of the data collection and treatment, who the recipients are and the bank holders where the data will be stored, about any data transfer, the term during which the data will be kept, among others. • Data subjects can refuse to provide their consent as a bulk or line by line. Additionally, they have the right to require the update, inclusion, modification and/or destruction of their personal data (as a bulk or line by line, as applicable) when the data is partially or totally inaccurate, incomplete, wrong, fake, or when the data is no longer necessary or pertinent to the purpose for which it was collected, or the agreed term to be processed has expired. • Consent must be previous, informed, express and unequivocal. Whenever there is sensitive data, consent must be in writing (either physically or electronically signed). However, we suggest to always obtain the consent in writing, and store the original document. The Data Protection Authority. However, the data subject can also oppose to any unauthorized data treatment or collection.
10	Who is responsible for the implementation of the law? • NRA? • Ministry of ICT?	Other.	The Peruvian Data Protection Authority, which is part of the Ministry of Justice and Human Rights.

#	Question	Response/Yes/No	Comments
	• Army (or affiliate)? • Other?		
11	Who is responsible for possible breaches to the law? • Users? • Service provider? • Local operator? Just for themselves, or also on behalf of their counterparts? • Foreign operator / data handler?	Data controllers and data processors.	Data controllers and data processors will be responsible for any breaches to the law, whenever Peru's data protection laws are applicable.
12	Implications of breach • Risks to companies – Penalties – Loss of license – Other • Risks to people		The breach of data protection obligations could lead to the following consequences: • Penalties by the Data Protection Authority. • Compensation for damages. • Criminal sanctions.

#	Question	Response/Yes/No	Comments
	– Penalties – Arrest – Other		
13	Who monitors the correct implementation of the law • Parliament? • Consumer associations / civil society? • Nobody? • Other?	Other.	The Peruvian Data Protection Authority.

Country: Uruguay

Questionnaire

#	Question	Response/Yes/No	Comments
1	What is the relevant legislation? Are general data protection laws the only relevant laws or are there other sector specific laws as well that may impose additional requirements?		In Uruguay, Act N° 18.331 regulates general data protection as well as its Reglamentory Decree N° 414/009. However, recently some significant requirements have been imposed by Section 37 of the Act N° 19.670 (National Budget Act), which basically modifies the scope of application of the Law. These modifications entered into force since January 1st, 2019.
2	Are there any bills currently before parliament, or expected to come before parliament, that propose to amend the existing regime?		Currently there is no bill before parliament.
3	What type of approach is this? • Consumer protection led? • Other?		The approach of the act N°18.331 is Consumer Protection Led, what it means the protection of the titular of the personal data.
4	What is the scope of the law?		In principle, the Act applies to all personal data, no matter the support of them (according to Section 3 of Act 18.331).

#	Question	Response/Yes/No	Comments
	• Telecoms? • Social media? • Media? • Medical? • Banking? • Other?		However, there are certain data basis that are expressly excluded from this regulation: • Data basis from natural person regarding their private or domestic activities. • Data basis which main purposes are national security, defence, State's security, among others. Data basis to be created by special regulation (Section 1 of the Decree 437/009). For instance, Decree 437/009 establishes that banking operations regarding investments, loans, mortgage, or any other credit operation, are excluded from the scope of application since it is specifically regulated.
5	What does it imply in terms of data collection? • Do all types of data need to be captured, or only personal data? How are they categorised? • Is the data stored by the commercial entity or by a public entity? • Is the data copied / sent to a public entity?		• According to Section 3 of the Act 18.331, the scope of application of the Act involves data basis registered in any kind of support. We understand that the name of the Act reflects that only personal data should be taken into consideration. The Act distinguishes different data basis: • Sensitive data; • Health care data; • Telecoms data; • Data transferred internationally; • Publicity data; • Commercial activities data; and

#	Question	Response/Yes/No	Comments
			• Where the data is stored by the commercial entity, in its data base. Section 17 of Act N°18.331, provides that personal data may be communicated to public entities, as long as the main aim of the personal data base is accomplished, and also the Prior Informed Consent of the titular of the data is taken into account.
6	What does it imply in terms of data storage? • Does data have to be stored locally? • Can data be stored outside of the country? • Can data stored locally be exported outside of the country? • Does that require an authorisation? • If so, by whom?		• Data may be stored locally, depending on the purpose of the data base. Additionally, the data shall be registered in a term of 90 days once the data base becomes operational. Otherwise, penalties are established. • Data can be stored outside of the country but under some conditions; for example: permissions for the control unit shall be granted, standards must be obeyed. • Data stored locally can be exported depending on the purpose of the data base. Moreover, depending on the type of data, permissions or authorizations shall be granted by the unit regulator “Regulatory and Control Agency of Personal Data"
7	What does it imply in terms of data processing? • Do the same processes apply to		• Data processing only applies to personal data, since the scope of both the Law and the Reglamentory decree is personal data.

#	Question	Response/Yes/No	Comments
	all data, or only to personal data? • Are these processes same for technical and commercial usage? • Can data be processed abroad? If so, does the data processor have to give mirror access locally? • How long is the data stored? • Is the data destructed after that period of time, or kept? • Is that monitored independently, or only by the State?		• Since the data base commercialization is forbidden by law, there is no technical and commercial usage. • According to Act N°18.331, Section 23, personal data is not allowed to be processed abroad. However, some exceptions are provided, for example: International Judicial cooperation, health data exchange, among others. • Yes, data can be processed abroad, but in most cases permissions and authorizations are required by law. • The data will be stored as long as the titular of the personal data and the database administrator maintain their purpose. Once the legal bond is extinguished, the data is destroyed. The aspects mentioned above are monitored by the State, specifically by the Regulatory and Control Agency of Personal Data", which is a unit regulator.
8	What does it imply in terms of data usage? • Can data be sold? • Can statistical data be sold?		None of this type of data is allowed to be sold.

#	Question	Response/Yes/No	Comments
	• Can technical data be sold?		
9	What control do people have on their data? • Are people informed of the data being collected? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) as a bulk? • Are people capable of accepting (= they want it) or rejecting (= they don't want it) line by line? • How is that approval stored? • Who monitors it?		• Yes, people are informed of the data being collected, according to Section 4, 5, 8, and 9 of Law N° 18.331. Moreover, the Prior Informed Consent is a fundamental principle in our legislation. • Yes, people are allowed by law to accept or deny their personal data being collected in any data base. • Yes. • The approval is stored in writing. • These aspects are monitored by the Regulatory and Control Agency of Personal Data".
10	Who is responsible for the implementation of the law?		Since data bases shall be registered, the "Regulatory and Control Agency of Personal Data" is responsible for the implementation of the law.

#	Question	Response/Yes/No	Comments
	• NRA? • Ministry of ICT? • Army (or affiliate)? • Other?		
11	Who is responsible for possible breaches to the law? • Users? • Service provider? • Local operator? Just for themselves, or also on behalf of their counterparts? • Foreign operator / data handler?		According to section 12 of Law N° 18.331, the database administrator is the individual responsible for possible breaches to the law.

#	Question	Response/Yes/No	Comments
12	Implications of breach • Risks to companies – Penalties – Loss of license – Other • Risks to people – Penalties – Arrest – Other		• According to Section 35 of Act N°18.331, some of the risks in case of breach for the data base responsible are; penalties, data base suspension for 5 days, warning, among others. However, the risks mentioned shall be applied considering the reaffirmation, recidivism of the violation committed.
13	Who monitors the correct implementation of the law • Parliament? • Consumer associations / civil society? • Nobody? • Other?		The “Regulatory and Control Agency of Personal Data monitors the correct implementation of the law.